NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTEGRATED CYBER DEFENSES:
TOWARDS CYBER DEFENSE DOCTRINE

by

Donald Wayne Cloud, Junior

December 2007

Thesis Co-Advisors: Daniel Moran
Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2007	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Integrated Cyber Defenses: Towards Cyber Defense Doctrine	5. FUNDING NUMBERS
6. AUTHOR(S) Donald Wayne Cloud, Junior	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

At the same time that the Department of Defense (DoD) has leveraged Network Centric Warfare concepts to increase the operational effectiveness of U.S. military forces and to gain decision superiority over adversaries, the DoD has become increasingly dependent upon the secure operations of computer networks and infrastructure. As a result, DoD computer network operations have become a vital center of gravity of U.S. military forces. Unfortunately, computer networks are growing faster than the DoD can defend them, while cyber attack sophistication and numbers of attacks continue to rise. In addition, many nation-states have begun to invest in developing real cyber warfare capabilities. Therefore, it is critical to U.S. military operations that the DoD has the capability to defend its own networks against aggressive adversaries.

Alarmingly, the DoD currently does not have a formal foundation for Computer Network Defense doctrine. All existing doctrine and regulations focus on computer and network security and not warfare. Another challenge in the development of effective doctrine with respect to cyber warfare is that we have little real historical experience of conducting it. However by leveraging the similarities of the air warfighting domain to that of the warfighting domain of cyberspace, this thesis will extrapolate historical doctrinal lessons regarding defensive air power doctrine to build a foundation for the development of Computer Network Defense doctrine.

14. SUBJECT TERMS CNO, CNA, CNE, CND, Computer Network Operations, Computer Network Attack, Computer Network Exploitation, Computer Network Defense, Network Warfare, NW Operations, Network Attack, Network Defense, NetA, NetD, NW Support, Cyberspace, Cyber Warfare, Cyber Attack, Cyber Defense, Cyber Weapons, Cyber Fortifications, Cyber Terrain, Doctrine	15. NUMBER OF PAGES 121
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INTEGRATED CYBER DEFENSES:
TOWARDS CYBER DEFENSE DOCTRINE

Donald W. Cloud, Jr.
Major, United States Air Force
B.S., United States Air Force Academy, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Author: Donald Wayne Cloud, Junior

Approved by: Daniel Moran
Thesis Co-Advisor

Dorothy Denning
Thesis Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

At the same time that the Department of Defense (DoD) has leveraged Network Centric Warfare concepts to increase the operational effectiveness of U.S. military forces and to gain decision superiority over adversaries, the DoD has become increasingly dependent upon the secure operations of computer networks and infrastructure. As a result, DoD computer network operations have become a vital center of gravity of U.S. military forces. Unfortunately, computer networks are growing faster than the DoD can defend them, while cyber attack sophistication and numbers of attacks continue to rise. In addition, many nation-states have begun to invest in developing real cyber warfare capabilities. Therefore, it is critical to U.S. military operations that the DoD has the capability to defend its own networks against aggressive adversaries.

Alarmingly, the DoD currently does not have a formal foundation for Computer Network Defense doctrine. All existing doctrine and regulations focus on computer and network security and not warfare. Another challenge in the development of effective doctrine with respect to cyber warfare is that we have little real historical experience of conducting it. However by leveraging the similarities of the air warfighting domain to that of the warfighting domain of cyberspace, this thesis will extrapolate historical doctrinal lessons regarding defensive air power doctrine to build a foundation for the development of Computer Network Defense doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS, ACRONYMS, AND SYMBOLS

AAA	Anti-Aircraft Artillery
AAM	Air-to-Air Missile
AB	Air Base
AF	Air Force
AFDD	AF Doctrine Document
AFI	AF Instruction
AO	Area of Operations
AOR	Area of Responsibility
C2	Command and Control
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	CJCS Instruction
CJCSM	CJCS Manual
CNA	Computer Network Attack (joint doctrinal term)
CND	Computer Network Defense (joint doctrinal term)
CNE	Computer Network Exploitation (joint doctrinal term)
CNO	Computer Network Operations (joint doctrinal term)
COCOM	Combatant Command
DoD	Department of Defense
DODD	DoD Directive
DODI	DoD Instruction
EAF	Egyptian Air Force (also referred to as the UARAF)
EADF	Egyptian Air Defense Force
FM	Field Manual
IA	Information Assurance
IAF	Israeli Air Force
IDF	Israeli Defense Forces
IFF	Identify-Friend-of-Foe
INFOCON	Information Operations Condition
INFOSEC	Information Security
IO	Information Operations

JFCC-NW	Joint Functional Component Commander-Network Warfare
JOA	Joint Operations Area
JP	Joint Publication
JTF-GNO	Joint Task Force-Global Network Operations
MCWP	Marine Corps Warfighting Publication
OPNAV INST	Operational Navy Instruction
NetA	Network Attack (AF doctrinal term synonymous with joint term CNA)
NetD	Network Defense (AF doctrinal term synonymous with joint term CND)
NetOps	Network Operations
NCW	Network Centric Warfare
NW	Network Warfare
NW Ops	NW Operations (AF doctrinal term synonymous with joint term CNO)
NW Support	NW Support (AF doctrinal term synonymous with joint term CNE)
RAF	Royal Air Force (United Kingdom)
RADAR	RAdio Detection And Ranging
RDF	Radio Detection Finding
SAM	Surface-to-Air Missile
STRATCOM	U.S. Strategic Command
SD	STRATCOM Directive
TNCC	Theater Network Control Center
TRO	Tailored Response Options
UARAF	United Arab Republic Air Force (also referred to as the EAF)
WWII	World War II
WWW	World Wide Web

ACKNOWLEDGMENTS

To God for giving me the opportunity and strength to do his works

To my Family for their love, support, and understanding

Christina Cloud
Bailee and Caleb

To my Co-Advisors for their guidance, mentoring, patience, and pragmatism

Professor Daniel Moran (National Security Affairs Department)
Professor Dorothy Denning (Defense Analysis Department)

To select NPS Instructors for teaching me how to "think" about the study of warfare

Professor (LT, USN Reserves) Mike Jones (Naval War College)
Professor Thomas Moore (Naval War College)
Professor Douglas Borer (Defense Analysis Department)
Captain (USN) Timothy Doorey (National Security Affairs Department)
Commander (USN) Michael Herrera (Information Warfare Department)
Professor Richard Grahlman (Naval War College)
Professor Jan Bremer (Naval War College)

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE AND RELEVANCE

The Department of Defense (DoD) continues to expand its Network Centric Warfare (NCW) capabilities leveraging U.S. advantage in computer network and information technologies in order to gain asymmetric battlefield advantage to get inside adversary decision cycles to shorten the "kill chain." As a force multiplier, NCW continues to increase the operational effectiveness of U.S. military forces; however as a consequence, U.S. military operations have become increasingly dependent upon the secure operations of DoD computer networks. Thus, DoD computer network operations have become a vital center of gravity of U.S. military forces.[1] Lieutenant General Robert Elder, the Commander of the 8th Air Force (the predecessor to Air Force (AF) Cyber Command), reinforced this assessment as follows:

> The Air Force now recognizes that cyberspace ops is a potential center of gravity for the United States and, much like air and space superiority, cyberspace superiority is a prerequisite for effective operations in all warfighting domains.[2]

At the same time, the proliferation of "cyber weapons" and cyber crime tools continues to increase, making them easier and cheaper to obtain, easier to use, more effective at defeating network defenses, and more dangerous.[3] Combined with the continuing negative trend that the number of successful infiltrations into government and

---

[1] *Information Operations Roadmap (DECLASSIFIED)*, Oct 30, 2003, http://freegovinfo.info//node/913, Last accessed Sept 11, 2007, 6 and Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress*, Updated Mar 15, 2007, Washington, DC: Congressional Research Service, 2007, 12-14.

[2] Lt Gen Robert Elder as quoted in Peter A. Bauxbaum, "Air Force Explores the Next Frontier," *GCN Magazine*, Feb 19, 2007 reprinted in *U.S. Air Force Aim Points*, Feb 21, 2007, http://aimpoints.hq.af.mil/display.cfm?id=16792, Last accessed Feb 21, 2007.

[3] Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Updated Jun 5, 2007, Washington, DC: Congressional Research Service, 2007, 11-12 and Graeme Wearden, "Price of Cybercrime Tools Shrinks," *ZDNet*, Feb 9, 2007, http://news.zdnet.com/2100-1009_22-6158025.html, Last accessed Feb 16, 2007.

civilian computer networks has been increasing at an alarming rate, adversary cyber operations pose an increasing threat to DoD networks, U.S. military operations, U.S. national security, and U.S. sovereignty.[4]

U.S. adversaries recognize that the DoD is dependent upon information superiority and critical information infrastructure; thus, many nations and organizations have demonstrated and continue to invest in their cyber attack capabilities.[5] In the assessment of the Office of the Secretary of Defense in 2003:

> Networks are growing faster than we can defend them…unprotected networks surrender asymmetric advantage…attack sophistication is increasing…[and the] number of [network] events is increasing.[6]

Therefore, the DoD and each U.S. military service faces the daunting challenge of determining how they should employ the most effective "capabilities to shape and defend cyberspace" against determined adversaries and mounting threats.[7]

B. LITERATURE REVIEW

To confront these cyber threats, the Joint Staff established Computer Network Operations (CNO) as one of five core capabilities within joint Information Operations (IO) doctrine.[8] Similarly at the service level, the AF published Network Warfare Operations (NW Ops) doctrine as one of four mission areas within AF Information Operations doctrine.[9] These doctrines state that joint and AF forces will perform the

[4]Rita Teehan, *Data Security Breeches: Context and Incident Summaries*, Updated May 7, 2007, Washington, DC: Congressional Research Service, 2007, 1-6.

[5] Charles Billo and Welton Chang, *Cyberwarfare: An Analysis of Means and Motivations of Selected Nation States*, Hanover, NH: Dartmouth College Press, 2004 and *Planning Considerations for Defensive Information Warfare - Information Assurance*. Falls Church, VA: Defense Information Systems Agency, 1993, 16-17.

[6] *Information Operations Roadmap (DECLASSIFIED)*, 44-45.

[7] *Quadrennial Defense Review Report*, Feb 6, 2006, Washington, DC: Office of the Secretary of Defense, 2006, 32, http://www.defenselink.mil/qdr/, last accessed Feb 8, 2007.

[8] *Joint Publication (JP) 3-13: Information Operations*, Feb 13, 2006, Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf, last accessed Feb 6, 2007.

[9] *Air Force Doctrine Document (AFDD) 2-5: Information Operations*, Jan 11, 2005, Washington, DC: Air Force Publishing, 2005, http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5/afdd2-5.pdf, last accessed Feb 6, 2007. In addition, "Computer Network Operations" (abbreviated CNO) in joint doctrine is synonymous with "Network Warfare Operations" (abbreviated NW Ops) in AF doctrine. For brevity, the joint term CNO will be used from this point forward in reference to both CNO and NW Ops.

mission of Computer Network Defense (CND)/Network Defense (NetD);[10] however, neither publication provides doctrinal guidance as to how military forces at the operational/campaign level should be employed to effectively defend DoD or AF networks to fend off cyber attacks while they are in progress. A survey of all joint publications (JPs) reveals that subordinate JPs exist for four of the five IO core capabilities;[11] however, a JP on CNO (and thus CND) is absent. A comparable survey of AF Doctrine Documents (AFDD) reveals the same gap--that is, an AF doctrinal publication on NW Ops (and thus NetD) is also missing. Furthermore, an exhaustive survey of DoD Directives (DODD), DoD Instructions (DODI), Chairman of the Joint Chiefs of Staff (CJCS) Instructions (CJCSI), CJCS Manuals (CJCSM), Air Force Instructions (AFI), Marine Corps Warfighting Publications (MCWP), Operational Navy Instructions (OPNAV INST), and Field Manuals (FM) reveals that an overwhelming preponderance of guidance focused on operational risk management methodologies to mitigate risks before cyber attacks occur by reducing vulnerabilities in information systems through information security (INFOSEC) programs, information assurance (IA) programs, certification/accreditation programs, and defense-in-depth architectures (see Appendix A for a list of the most current and relevant DoD publications on this topic). The sum of these measures equates to building, designing, and maintaining information systems and infrastructure that are less vulnerable to and more fortified against cyber attacks; however, these pre-attack measures do not provide guidance on how to wage an effective CND campaign against a determined adversary during attacks. The only two reference to CND responses to cyber attacks in progress are 1) one-half of a page of text acknowledging that DoD components shall develop and execute courses of action in response to network attacks[12] and 2) clarification that Joint Task Force-Global Network Operations (JTF-GNO) and/or subordinate commanders will develop Tailored Response

[10] "Computer Network Defense" (abbreviated CND) in joint doctrine is synonymous with "Network Defense" (abbreviated NetD) in AF doctrine. For brevity, the term CND will be used from this point forward in reference to both CND and NetD.

[11] The five core IO capabilities Electronic Warfare (EW), Computer Network Operations (CNO), Operational Security (OPSEC), Military Deception (MILDEC), and Psychological Operations (PSYOP)

[12] *DODI 8530.2: Support to Computer Network Defense (CND)*, Mar 9, 2001, Washington, DC: Office of the Secretary of Defense, 2002, 22 and 32, http://iase.disa.mil/policy.html, last accessed Feb 20, 2007.

Options (TROs) to respond to specific intrusion characteristics.[13] However, these references provide no doctrinal clarity or details regarding how those courses of action should be developed or executed.

An expanded survey of scholarly works and other government documents reveals that these works fall into two broad categories. The first category includes publications that focus on cyber warfare at the strategy and policy level (see Appendix B for a list of the most current and relevant publications on this topic). These publications address policy recommendations, decisions, and evolutions at the national/grand strategic level aimed at strategically posturing the United States to leverage and protect cyberspace in order to protect U.S. national interests. In the area of CND, these publications discuss policies aimed at reducing the vulnerability of critical infrastructure and information systems before cyber attacks occur and/or enhancing recovery capabilities after cyber attacks have occurred; however, these documents do not address the best operational/campaign-level framework for defending against and repelling cyber attacks while they are occurring. The second category of publications focuses on cyberwarfare tactics, techniques, and/or tools (see Appendix B). These publications discuss specific methods or tools (such as encryption, anti-virus, biometrics, access controls, filters, and intrusion detection, backup and recovery, etc.) that can be employed to reduce the vulnerability of information systems before cyber attacks occur and/or to enhance recovery capabilities after cyber attacks have occurred. However, these documents also fail to address the best operational/campaign-level framework needed to defend friendly networks against cyber attacks in progress. Only one scholarly document provides a methodology for CNO; however, it only covers computer network attack (CNA) and computer network exploitation (CNE) mission areas and explicitly leaves out the mission area of CND, stating that "the significant task of how to defend against an attack will not be addressed in this paper."[14] In summary, this body of knowledge fails to answer one

[13] *Strategic Command Directive 527-1 (SD 527-1): Department of Defense Information Operations Condition (INFOCON) System Procedures*, Jan 27, 2006, Offutt Air Force Base, NE: Headquarters U.S. Strategic Command (USSTRATCOM), 2006, https://infosec.navy.mil/pub/docs/documents/dod/dodd/stratcom_d527-011_infocon_20060127.pdf, last accessed Feb 16, 2007.

[14] Juan Carlos Vega, *Computer Network Operations Methodology*, Monterey, CA: Navy Postgraduate School, 2004.

very basic question: At the operational level of war, how should U.S. military forces be employed to fight an effective CND campaign against determined, active, and adaptive adversaries when they attack friendly computer networks? To bring this question into tighter focus for the AF, how should AF network defense forces be employed to fight an effective CND campaign across all AF networks against determined, active, and adaptive adversaries at the operational level of war?

C. METHODOLOGY

One of the difficulties in the development of effective doctrine with respect to cyber warfare is that we have little experience conducting it. Our understanding of its conduct is necessarily based to a large extent on theoretical speculation and hypothetical scenario-building. As General Ronald E. Keys, Commander of the AF's Air Combat Command, so eloquently stated when describing the AF's new Cyber Command and calling cyberspace the AF's new high frontier, "this is about warfare, not about novelty."[15] Therefore, drawing upon the similarities between the warfighting domain of cyberspace to that of the air domain (e.g. speed of operations, distance of effects, vastness of areas of operations (AOs), permeability of borders/boundaries, degrees of freedom/maneuver, difficulty in building massive fortifications, etc.), this thesis will answer the research question above through a comparative case study comparing and contrasting the conduct of a CND campaign today with that of two historical air defense campaigns. In both forms of warfighting, it is apparent that operational level command-and-control (C2) relationships, operational employment, and technology employment are important factors to the effectiveness or ineffectiveness of defensive doctrine and campaigns at the operational level of war. The major argument of this thesis is that the proper combination of operational level C2, operational employment, and technology employment are sufficient to explain the effectiveness or ineffectiveness of air defense campaigns and thus computer network defense campaigns.

[15] Gen Ronald E. Keys as quoted in Erik Holmes, "Wynne Is Pleased with Tanker 'Horse Race'"*Air Force Times*, Feb 26, 2007, 10.

The major questions that this thesis will answer are 1) how analogous are the domains of cyberspace and airspace and how are they different, 2) how does operational level C2 impact the effectiveness of defensive campaigns, 3) how does operational employment impact the effectiveness of defensive campaigns, and 4) how does technology employment impact the effectiveness of defensive campaigns?

Chapter II will focus on comparing and contrasting the domains of airspace and cyberspace in order to establish more clearly the extent to which the warfighting properties of cyberspace are conceptually similar to those of airspace. Then, historical case studies regarding operational level defensive air campaigns will be analyzed in Chapters III and IV. The two cases that have been selected are the British defensive air campaign during the Battle of Britain in 1940 and the Egyptian defensive air campaign during the Six Days War in 1967. The Battle of Britain was selected because it represents the first modern air campaign; furthermore, British air power doctrine was battle-tested during this campaign with positive results (e.g. the successful defense of the United Kingdom against the invasion of German military forces).[16] On the other end of the spectrum, the Six Days War represents an air campaign in the jet and missile age; furthermore, Arab air power doctrine was battle-tested during this campaign with negative results (e.g. the failed defense of the Egypt against Israeli invasion).[17] Both

[16] Len Deighton, *Battle of Britain*, London, UK: George Rainbow Limited, 1980; "The Battle of Britain Toolkit," (Air Command and Staff College Project 97-0564.01 updated Apr 28, 2001), *Air Command and Staff College Distance Learning CD version 3.2*, Maxwell AFB, AL: Air University Press, 2003; Richard Overy, *The Battle of Britain: The Myth and the Reality*, New York, NY: W. W. Norton & Company, 2000; T.P. Gleave, "The Battle of Britain: Strategy, Tactics, Atmosphere," *Flight International*, September 16, 1965, 494-502; John Monsarrat, "Radar in Retrospect, How It Helped Win the Battle of Britain and the Battle of Okinawa," *Journal of Electronic Defense*, 14-10, October 1991, 92-100; Sir Hugh Trenchard, "Air Power and National Security," *Royal Air Force Pamphlet*, August 1946; Sir Hugh Trenchard, "The Principles of Air Power in War," *Air Power, Three Papers by the Viscount Trenchard*, Paper Two: 18-28, May 1945; *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007; and *The Battle of Britain Historical Society*, http://www.battleofbritain.net/, last accessed Feb 6, 2007.

[17] Michael Oren, *Six Days of War: June 1967 and the Making of the Modern Middle East*, Oxford, UK: Oxford University Press, 2002; Kenneth M. Pollack, "Air Power in the Six-Day War," *The Journal of Strategic Studies* 28, No. 3, June 2005, 471-503; Kenneth M. Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, Lincoln, NE: University of Nebraska Press, 2002; Stanley S. Gunnersen, *A Study of Airpower Employment in the Six Days War*, Maxwell AFB, AL: Air University, 1971; John F. Kreis, *Air Warfare and Air Base Air Defense, 1914-1973*. Washington, DC: Office of Air Force History, U.S. Air Force, 1988, 306-319; Lon O. Nordeen, Jr. *Air Warfare in the Missile Age*, Washington, DC: Smithsonian Institution Press, 2002, 111-123; Leo Heiman, "Soviet Air Tactics—No Room for Initiative," *Air Force Magazine*, 51, Aug 1968, 42-45.

cases shall be analyzed in order to glean key insights as to how operational command and control, operational employment, and technology employment contributed to or detracted from the effectiveness of each respective air defense campaign.

For clarity, cyber warfare discussions in Chapter II and air warfare discussions in Chapters III and IV will be purposefully kept separate within these respective chapters in order to avert confusion of the facts and propositions (e.g. cyber warfare will not be discussed in Chapters III and IV). Then, Chapter V will fuse the observations from Chapters II, III, and IV in order to build the base proposals for Computer Network Defense doctrine. The successful lessons from the Battle of Britain and the failed lessons from the Six Days War will be combined in the context of the doctrinally significant attributes of the warfighting domain of cyberspace. Analogy shall be used to develop a thought experiment for what the first real cyber war might look like in order to clarify how these CND doctrinal propositions would apply.

The thesis will close with a recommendation to the AF to build a system correlating to successful historical employments of integrated air defenses of the past to answer the question "how should AF network defense forces be employed to fight an effective CND campaign across all AF networks against determined, active, and adaptive adversaries?" The findings of this research will be used to make specific recommendations regarding the desirable characteristics of integrated cyber defenses, conceived by analogy with successful integrated air defenses of the past. The emphasis, as has been proposed, will be on operational level C2, operational employment, and technology employment to effectively fuse network defensive capabilities across platforms. The findings of this research will help set the stage for a draft CND doctrinal framework and may inspire further doctrinal research to begin filling the CND doctrinal gap across the DoD. Finally, this proposed CND methodology can be combined with Juan Vegas aforementioned proposed CNO framework[18] (that covers the CNA and CNE mission areas) to provide starting point for doctrinal discussions on CNO, CNA, CNE, and CND with the objective of publishing a new joint doctrinal publication.

[18] Juan Vega, *Computer Network Operations Methodology*.

THIS PAGE INTENTIONALLY LEFT BLANK

II. AS A WARFIGHTING DOMAIN, WHAT IS CYBERSPACE?

A. CYBERSPACE — THE NEW "HIGH FRONTIER?"

Lieutenant General Robert Elder, the Commander of the 8th Air Force (the predecessor to AF Cyber Command), captured the core challenge facing the AF and the DoD regarding warfare in cyberspace when he stated:

> For [the AF], one of the big things was understanding what the cyberspace domain is and then what operations in cyberspace means .... how cyberspace could be used to enhance our contributions to a joint fight.[19]

Before military policymakers can decide how to best organize, train, and equip a viable military force that can conduct decisive operations in cyberspace, they must have a fundamental and common understanding of what cyberspace is as a warfighting domain. Military strategists take for granted their common understanding of the classical warfighting domains of air, land, sea, and space as well as what their key attributes are in reference to warfighting; furthermore, military doctrine for each of these domains is uniquely adapted and updated to best leverage these attributes to gain military advantage on the battlefield. The warfighting domain of cyberspace, in contrast, lacks this basic definition, understanding, or identification of key attributes. Without this foundation, the prefix "cyber" has been haphazardly and inappropriately attached to many military terms with detrimental effects to effective doctrinal debates about warfare in cyberspace.

This chapter will rectify this problem by answering the question "as a warfighting domain, what is cyberspace?" Second, it will expound upon this basic definition by clarifying key related military terms as they pertain to warfighting in cyberspace. Finally, this chapter will initially assess the doctrinal implications for warfighting in cyberspace based upon this working definition.

[19] Lt Gen Robert Elder as quoted in SSgt C. Todd Lopez, "Fighting in Cyberspace Means Cyber Domain Dominance," *AF Print News*, Feb 28, 2007, http://www.af.mil/news/story.asp?id=123042670, last accessed Sept 11, 2007.

B. ASSUMPTIONS

To scope the problem of defining cyberspace as a warfighting domain, analysis will be purposefully limited to the perspective of military warfighters currently tasked with primary responsibility for combat operations in cyberspace, to include the Combatant Commander of U.S. Strategic Command (STRATCOM), the Commander of Joint Task Force-Global Network Operations (JTF-GNO), the Joint Functional Component Commander for Network Warfare (JFCC-NW), and related service component commands. In addition, analysis will be focused at the operational level of war in the context of conventional warfare (state versus state; military versus military). This level of analysis affords more fruitful discussions regarding operational art, doctrine, and military capabilities, whereas the tactical level would drive the discussion towards tactics, techniques, procedures and technical details. Likewise, the strategic level would lend itself to policy discussions vice doctrinal analysis. Within this warfighting analytical framework, actors in cyberspace will be categorized as combatants or non-combatants, and as such, the Laws of Armed Conflict apply. In keeping with current legal interpretations of the Laws of Armed Conflict, combatants and non-combatants must be people, and thus botnets, zombienets, etc. cannot be combatants any more than a jet or a tank can. In summary, the following analysis will evaluate an operational level commander's perspective of what cyberspace is as a warfighting domain and how he/she would likely employ military forces to conduct campaigns and operations in cyberspace.

C. CYBERSPACE — A BASIC DEFINITION

In 1984, the term *cyberspace* first appeared in the science fiction work *Neuromancer* where the author described cyberspace as:

> A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.[20]

[20] William Gibson, *Neuromancer*, New York, NY: Ace Books, 1984, 69.

Since then and in concert with the boom of the Internet and World Wide Web (WWW) in the 1990s, the term *cyberspace* has most often been used as a metaphor for a virtual world created by computers[21] and is typically used synonymously in reference to the Internet or the WWW. This misinterpretation has even been captured in DoD doctrine which defines cyberspace as "the notional environment in which digitized information is communicated over computer networks."[22]

A virtual, notional, or metaphorical definition of cyberspace presents two key problems. First, it is difficult to build real military capability or conduct real military operations in a domain that doesn't really exist. Second, this definition cannot explain the measurable, real-world impacts of events in cyberspace such as computer systems breached, identities stolen, lives affected, time/work/data destroyed or compromised and associated monetary impacts, cascading electrical grid outages, airline flights delayed, "cyber wars,"[23] etc. Also, cyberspace is comprised of physical, engineered components and produces both positive and negative effects in the physical world. Information content and information flow are also real. Signals, bits, and bytes are all real, measurable phenomena. Therefore, cyberspace is not a metaphor, virtual world, notional environment, or hallucination. Cyberspace is real and must be defined in real terms.

Throwing out myriad metaphorical definitions of cyberspace, the most useful and complete definition of *cyberspace* as a warfighting domain that is currently available is:

> A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures.[24]

---

[21] Libicki, Martin C. *Defending Cyberspace and Other Metaphors*. Washington, DC: National Defense University, 1997.

[22] *Joint Publication (JP) 1-02: Department of Defense (DoD) Dictionary of Military and Associated Terms*, Apr 12, 2001 (as amended through Jan 12, 2007), Washington, DC: Office of the Chairman, Joint Chiefs of Staff (CJCS), 2007, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, last accessed Sept 11, 2007.

[23] Such as the Palestinian-Israeli, China-United States, and Russia-Estonia Cyberwars, for example.

[24] *AF Operational Concept – Cyberwarfare (DRAFT)*, Apr 1, 2007, San Antonio, TX: 67th Network Warfare Wing, 3.

Put another way, the cyberspace domain is "the maneuver space of the electromagnetic spectrum."[25] This definition is based upon real/physical elements of electronics and the electromagnetic (EM) spectrum. Examples of the real components that comprise cyberspace are visualized in Figure 1.

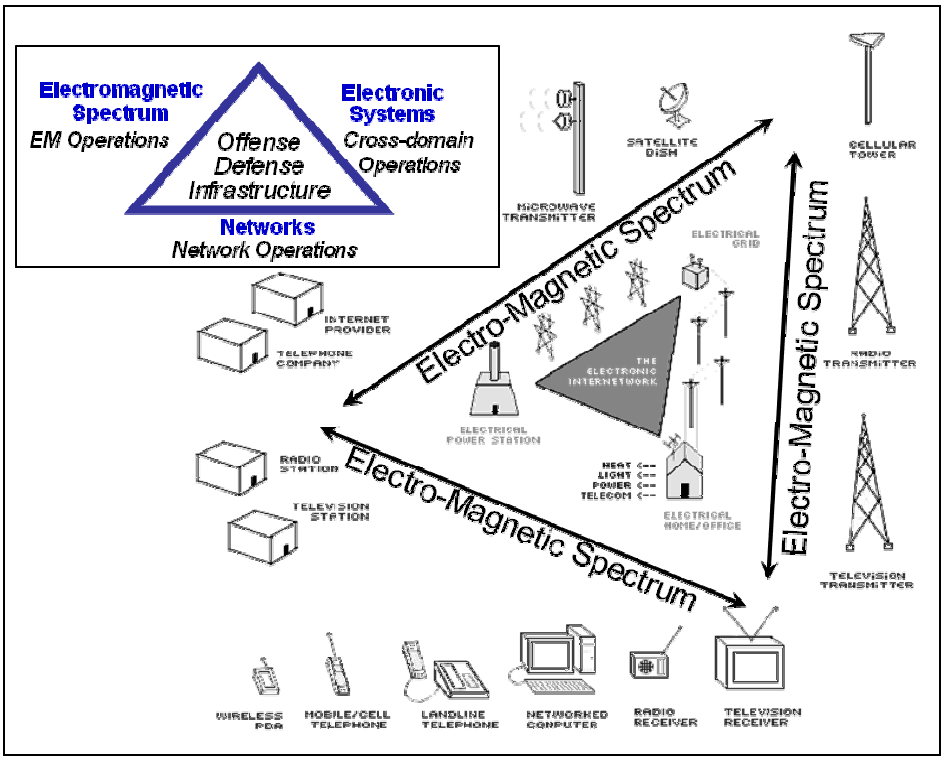


Figure 1. Activities and Systems in the Cyber Domain (From [26])

This definition effectively captures the core components of cyberspace to include electronics, infrastructure, data flow, and content as encoded and processed in cyberspace. It also provides a good starting point to further explore the robustness of this definition and to establish the basic attributes of cyberspace in order to set a proper foundation upon which to conduct further doctrinal analysis.

[25] Dr. Lani Kass, Director of the USAF Cyberspace Task Force, in Henry S. Kenyon, "Task Force Explores New Military Frontier," *Signal Magazine*, 61, No. 2, Oct 2006, 56.

[26] Figure 2.1, *AF Operational Concept - Cyberwarfare (DRAFT)*, 3.

D. DOCTRINALLY SIGNIFICANT ATTRIBUTES OF CYBERSPACE

An analytical framework is needed to properly dissect and establish the basic attributes of cyberspace in terms consistent with our current understanding of the classical warfighting domains of air, land, sea, and space. Milan Vego, a professor at the Naval War College, provides a simple yet useful framework for analyzing operational level warfare in terms of the critical factors of *space*, *forces*, and *time*.[27] Combined with the Naval War College chart in Table 3 of Appendix C, which compares some key features of the warfighting domains of air, land, and sea, this framework can be expanded to compare and contrast the key attributes of all warfighting domains. The dominant attributes which impact military operations in *space* are terrain, dimensions and degrees of freedom/maneuver, physical laws, and obstructions. The two most common military instruments used by *forces* to conduct military operations in said space are weapons to attack the adversary and fortifications to protect against adversary aggression. Adding the factor of *time*, military forces in space conduct operational movements and operational maneuvers over time with the objective of defeating the adversary on the battlefield. In conducting operational movements and maneuvers, the range and speed of both opposing forces and their weapons in each domain become significant factors. In summary, the doctrinally significant factors of any warfighting domain are terrain, dimensions and degrees of freedom/maneuver, physical laws, weapons, fortifications, operational movements, operational maneuvers, range, and speed. Using the table in Appendix C as a model, core attributes for the air, land, sea, and space warfighting domains can be derived to create Table 1. Furthermore, this table identifies the key questions that must be answered in order to build a fundamental doctrinal understanding of cyberspace as a warfighting domain (see empty far right column).

[27] Milan Vego, *Operational Warfare*, Newport, RI: Naval War College, 2000, 29-103.

Domain	Land	Sea	Air	Space	Cyberspace
Made of	Earth	Water	Air	Vacuum	?
Lead Service	Army	Navy	Air Force	Air Force	?
Operational Doctrine and Developments	METT-T … Future Combat System & Future Force Warrior	Power Projection & Sea Control … Sea Shield, Sea Strike & Sea Basing	Global Reach/Power, Air Superiority (Tenants of Air Power) … Interdependent Fight	Operational Responsive Space and Space Superiority	?
Dominant Physics Governing Movement	Gravity and Friction	Gravity, Buoyancy, and Fluid Dynamics	Gravity and Aerodynamics	Gravity and Orbital Mechanics	?
Physical Dimensions & Degrees of Freedom	2 (fwd-back, left-right)	2 or 3 (fwd-back, left-right, up-down [subsurface])	3 (fwd-back, left-right, up-down)	3 (fwd-back, left-right, up-down)…constrained to orbital mechanics	?
Natural Obstructions to Movement	Elevation, Bodies of Water, and Rough Terrain	Bodies of Land and Shallow Water	Air Density and Elevated Terrain (Mountains/Hills)	Atmosphere	?
Combat Range/Radius	Tens to Hundreds of miles	Thousands of miles	Hundreds to Thousands of miles	Tens of thousands of miles+	?
Movement Speed	0-50 mph	0-50 knots	0-Mach 2+	0-35K mph+	?
Forces, Weapons, and Fortifications (Typical examples)	Infantry (Guns, Grenades, Mortars, RPGs), Artillery (Cannons, Rockets, Missiles), Tanks (Guns, Cannons, Rockets), Helicopters (Guns, Rockets, Missiles), Armor, Barricades, Physical Fortifications	Ships, Submarines, Hovercraft, Patrol Craft (Machine Guns, Cannons, Missiles, Rockets, Depth Charges), Armor	Fighters, Bombers, Helicopters (Machine Guns, Cannons, Missiles, Rockets, Bombs), Cruise Missiles, Hardened shelters, Revetments	Satellites, Rockets, Missiles	?

Table 1. Warfighting Domain Analytical Framework

1. Terrain in Cyberspace

In military context, *terrain* is defined as "a piece of ground having specific characteristics or military potential."[28] Furthermore, *terrain analysis* is defined as "the collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations."[29] Based upon these definitions, terrain should impact operations in cyberspace just as it impacts operations in the other four classical warfighting domains. Terrain provides the space in which forces operate, impacts the operations of said forces, delineates friendly/enemy/neutral territory, and encompasses combatants and non-combatants. A basic understanding of the terrain of cyberspace is necessary to any credible doctrinal discussion on this domain.

[28] Dictionary.com, *WordNet® 3.0*. Princeton University, http://dictionary.reference.com/browse/terrain, last accessed Sept 10, 2007.

[29] *JP 1-02*, 541.

Per the basic definition of cyberspace, *cyberspace* is made of electronics and the EM spectrum to store, modify, and exchange data via networked systems and associated infrastructures.[30] Furthermore, electronics and EM spectrum can be further subdivided into two broad categories: analog and digital.

For EM signals, the rules governing movement and maneuver are dictated by the laws of physics relating to the signal propagation of EM energy waves, whether it is radio waves, electrical pulses, laser light, etc. and regardless of transmission medium.[31] These laws are constant throughout the universe and apply to all EM signals within and traversing between electronics through any medium. As such, the degrees of freedom and maneuver for EM signals is 3-dimensional, the range is limited by the power of signal, and natural obstructions come in the form of physical obstructions to signals (line of sight obstructions, Faraday cages, breaks in communications lines, interference, etc.). These variables are captured in the various forms and derivations of the radar range equation. All EM signals travel at speeds close to that of the speed of light.[32] The combat radius or range of these signals is directly associated with the location of the transmitter source and receivers, the strength or power of the signal being transmitted, the loss of the signal as it traverses the medium (air, copper, space, fiber, etc.), and the capability of the receiver to discern the signal from noise. This range can be extended by networking EM switching devices to create long distance connectivity (e.g. telephone networks, the Internet, etc.). As such, natural obstructions come in the form of breaks in the connectivity established by networks. Today, this type of connectivity spans much of the globe (like in the WWW) and extends the combat radius or range for cyber operations to the global scale. Based on current human understanding of physical laws, the physics governing EM signals are non-changing and non-negotiable.

In order to extend human senses and communications beyond the limits of our physical bodies, engineers have leveraged EM physics to create rules that enable electronics to store, process, and exchange information. These rules give EM waveforms

[30] *AF Operational Concept - Cyberwarfare (DRAFT)*, 3.

[31] Richard A. Poisel, *Introduction to Communication Electronic Warfare Systems*, Boston, MA: Artech House, 2002, 19-52.

[32] Note: The specific speed that a waveform traverses a medium is affected by the medium itself, but for general purposes, EM signals propagate at approximately the speed of light.

human meaning such as the encoding of ones and zeroes into the frequency, amplitude, or phase of an EM signal for digital electronics. Examples include but are not limited to Institute of Electrical and Electronics Engineers (IEEE) standards (like IEEE 802.11 for Ethernet or IEEE 802.11g for wireless Ethernet), operating systems (like Windows XP, Mac OS, or Unix), network operating systems (like Cisco), network protocols (like TCP/IP [Transmission Control Protocol/Internet Protocol]), programs, programming languages (like C++, Java, ActiveX, Hypertext Markup Language [HTML]), database protocols (like Standard Query Language [SQL]), etc. These rules are not unlike those governing other warfighting domains such as air traffic control rules, driving rules, sea navigation rules, etc. The Open Systems Interconnect (OSI) model provides a useful framework for categorizing these rules as they pertain to communications (see Figure 2). All electronics were built by humans, and these rules were built into them. Since these are human-made rules, they can be changed by replacing or updating hardware and/or software. Unlike the physical laws, these rules can sometimes be bent or broken.

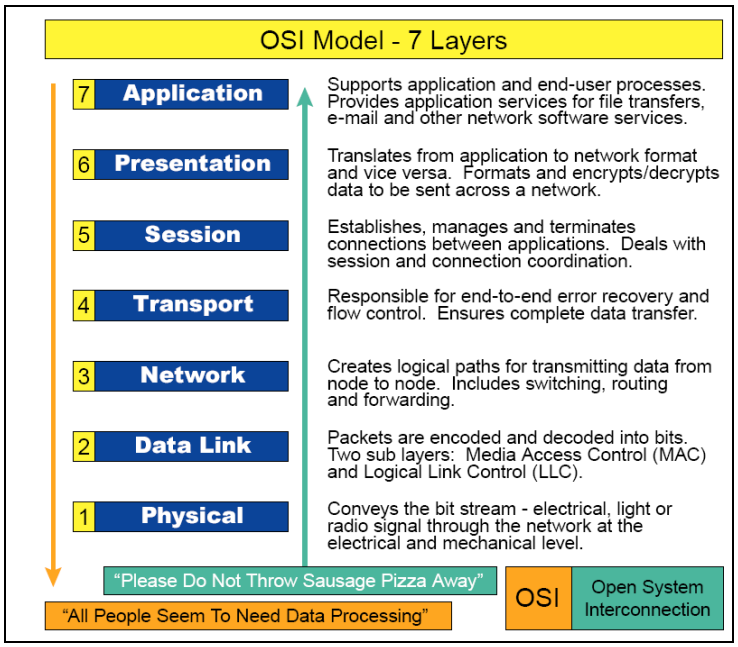


Figure 2. OSI Model (From [33])

[33] "OSI Model," *Huffman Reference Materials*, http://www.huffmanreference.com/pdf_download.html, last accessed Nov 20, 2007.

2. Weapons in Cyberspace (Cyberweapons)

In the classical warfighting domains, military forces employ weapons in order to attack or defend against an adversary. This is no different in cyberspace; however, the term *cyberweapon* has been utilized in many circumstances where it is inappropriate and/or inaccurate. Such misuse characterizes almost everything as a cyberweapon and thus nothing is a cyberweapon. What is required is a return to a foundational definition of *weapon* as **"**any instrument or means which is used for one's own [defense] or for attacking others."[34] Closely related, a *weapon system* is defined as "a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment required for self-sufficiency."[35] Examples of classical weapons and weapon systems are knives, guns, cannons, missiles, rockets, electronic warfare jammers, anti-aircraft artillery, tanks, fighter aircraft, bombers, warships, bombs, mines, weapons of mass destruction, etc. In several select cases, the term *weapon* is preceded by a particular domain in which said weapon is primarily employed, such as an *air weapon* or *space weapon*. To ensure the term *cyberweapon* is used properly, it is necessary to further define the key attributes that distinguish a weapon from other implements of war.

A simple "ready, aim, fire" test can be used to quickly determine whether or not an object is a weapon; note that the object must pass all three criteria to be a *weapon*. For the "ready" test, the object must be deliberately employed by a person or persons (typically a combatant). For the "aim" test, the object must be designed to target an adversary with the intent to cause harm. For the "fire" test, the object must transfer mass and/or energy to said adversary target with the intent to cause damage such as injury, death, destruction, disruption, blinding, etc. A weapon can be used for attack and/or defensive purposes, and a weapon is typically technological in nature.

Using this definition, an initial list of *cyberweapons* in existence today can now be derived to include logic bombs; Domain Name Service (DNS) attack code; Denial of Service (DoS) and Distributed Denial of Service (DDoS) code; malicious logic (Trojans, Viruses, Worms, Bots/Botnets/Zombies, hacking scripts, etc.), vulnerability exploitation

---

[34] Dictionary.com, *Kernerman English Multilingual Dictionary*, K Dictionaries Ltd., http://dictionary.reference.com/browse/weapon, last accessed Sept 9, 2007.

[35] JP 1-02, 582.

code, along with existing electronic warfare weapons like communications jammers.[36] *Cyberweapons* are as real as their classical counterparts. Note that the attacks and end effects themselves are not weapons but are instead the damage caused by weapons. For example, operators cannot "fire" a web defacement, DoS, or remote system shutdown; instead, they can "fire" a weapon in the form of malicious code, scripts, etc. that can result in these damaging effects.

3. Fortifications in Cyberspace

In the classical warfighting domains, military forces build fortifications in order to fend off adversary forces in order to protect friendly forces, territory, or targets. *Fortifications* are defined as "military works constructed for the purpose of strengthening a position."[37] Classical examples include walls, fences, fortresses, castles, star bastions, De-Militarized Zones (DMZs), moats, no-mans-land, mine fields, and so forth.[38] Key attributes that distinguish fortifications from weapons include: 1) they establish a defensive perimeter and control access into the perimeter (allowing friendly forces to enter and exit while preventing adversaries from entering), 2) they are often used to bolster the defensibility of the existing terrain, especially if the terrain is flat, 3) they are designed to absorb damage so as to protect what is inside, 4) they are often designed to employ patrols and weapons in such as manner as to maximize the effectiveness of the friendly weapons against an attacking force, and 5) said defenses can be layered (referred to as defense-in-depth). Based upon this definition, the following items in cyberspace are fortifications (and not weapons): firewalls, proxy servers, web and spam filters, mail relays, antivirus/antimalware software, router Access Control Lists (ACLs), cryptography and encryption, user access controls (such as Username/Password authentication, Public Key Infrastructure (PKI), Certificates, access cards, group policies, digital signatures,

---

[36] This list of example cyberspace weapons was derived and consolidated from multiple sections in Dorothy E. Denning, *Information Warfare and Security*, Berkeley, CA: ACM Press Books, 1999. This is not an all inclusive list.

[37] Dictionary.com, *Dictionary.com Unabridged (v 1.1)*, Random House, Inc., http://dictionary.reference.com/browse/fortification, last accessed Sept 9, 2007.

[38] Thomas J. Pingel, "Key Defensive Terrain in Cyberspace: A Geographic Perspective," *Proceedings of the 2003 International Conference on Politics and Information Systems: Technologies and Applications*, Orlando, FL, 2003, 159-163, http://www.geog.ucsb.edu/~pingel/, last accessed Aug 6, 2007.

etc.).[39] In the analog realm, fortifications also include anti-jamming, shielding, jam resistance, and so forth. Cyberspace fortifications are as real as their classical counterparts, and cyberspace fortifications are not to be confused with cyberweapons.

4. Reconnaissance and Movement in Cyberspace

Operational movement in cyberspace is dictated by the characteristics of the cyberspace domain. For example, travel through IP-enabled (Internet Protocol-enabled) portions of cyberspace is governed by various rules at the first four layers of the OSI model such as TCP/IP (Transmission Control Protocol/Internet Protocol) and the correlating physical layer and data link layer IEEE standards. Since EM signals travel at approximately the speed of light, adversary forces can conduct extremely long-range reconnaissance in cyberspace against enemy cyberspace targets. This long-range reconnaissance is akin to having U-2s, Globalhawks, and Predators with sensors capable of seeing the other side of the globe. Cyberspace reconnaissance can be conducted solely in cyberspace; however, a more effective approach would be to use all source intelligence to collect information across all domains against key cyberspace targets in preparation for attacks. The all source method is already used across the four classical warfighting domains, and no credible reason presents itself to not follow suit with cyberspace. At first glance, it would seem that reconnaissance in cyberspace would provide equal opportunities for both friendly and adversary forces; however, cyberspace provides nearly limitless fast avenues of approach, making the discovery of adversary reconnaissance difficult and challenging. Reconnaissance by fire techniques can also be used to probe fortifications and defenses for weaknesses. Finally, automation can help speed the process of probing defenses for weaknesses.

Once sufficient information is collected, an adversary can conduct operational maneuvers to launch an attack campaign through cyberspace via many avenues of approach. Since combined arms tactics are doctrinally accepted as the best method of employing military force, the same should hold true for employing forces in cyberspace.

[39] This list of example cyberspace fortifications was derived and consolidated from multiple sections in Dorothy E. Denning, *Information Warfare and Security,* Berkeley, CA: ACM Press Books, 1999. This is not an all inclusive list.

Once cyberspace defenses have been compromised and a military installation infiltrated (in cyberspace, as well as in the other four domains), enemy forces have just maneuvered into friendly cyberspace. From this point forward, the infiltrating force must systematically navigate, defeat, or circumvent any active and passive defenses to continue the assault. Of note, the defending force may be completely unaware that the attack has even happened as long as the attacker has not triggered any alarms or been spotted by patrols (if they have any). Once access to primary targets has been gained, the adversary can deliver the payload, whether it is destruction, disruption, exfiltration of intelligence, deception, usurping command and control, etc. either for the effect alone or better yet in support of combined arms tactics for a larger offensive campaign.

If the defending force detects the assault, then defenders have some options. The Defend-Relocate-Augment-Withdraw-Delay (referred to in military doctrine as DRAWD) provides a general defensive framework to counter an attack. Defenders can defend by building up additional fortifications (such as updating firewalls to block IP addresses, updating proxy servers to block web sites, etc.) and/or patching holes in the fortifications (updating antivirus on outdated systems and running antivirus scans), relocating network segments or moving to different portions of EM spectrum (for example, switching frequencies, satellite channels, and the like), withdrawing by shutting down or disconnecting machines or entire network segments, or delaying attackers with a mixture of the above methods. The offensive option, which would be available during times of war, would involve employing an attacking force to destroy or disrupt the adversary at their bases of operations or forward operating bases in cyberspace.

Domain	Land	Sea	Air	Space	Cyberspace
Made of	Earth	Water	Air	Vacuum	**Electronics & Electromagnetic (EM) Spectrum**
Lead Service	Army	Navy	Air Force	Air Force	**None**
Operational Doctrine and Developments	METT-T … Future Combat System & Future Force Warrior	Power Projection & Sea Control … Sea Shield, Sea Strike & Sea Basing	Global Reach/Power, Air Superiority (Tenants of Air Power) … Interdependent Fight	Operational Responsive Space and Space Superiority	**None**
Dominant Physics Governing Movement	Gravity and Friction	Gravity, Buoyancy, and Fluid Dynamics	Gravity and Aerodynamics	Gravity and Orbital Mechanics	**EM Physics**
Physical Dimensions & Degrees of Freedom	2 (fwd-back, left-right)	2 or 3 (fwd-back, left-right, up-down [subsurface])	3 (fwd-back, left-right, up-down)	3 (fwd-back, left-right, up-down)…constrained to orbital mechanics	**3 (fwd-back, left-right, up-down)**
Natural Obstructions to Movement	Elevation, Bodies of Water, and Rough Terrain	Bodies of Land and Shallow Water	Air Density and Elevated Terrain (Mountains/Hills)	Atmosphere	**Physical Obstructions to Signal Propagation, Breaks in Connectivity, Bandwidth and Throughput Constraints**
Combat Range/Radius	Tens to Hundreds of miles	Thousands of miles	Hundreds to Thousands of miles	Tens of thousands of miles+	**Signal Power (Extended by Network Connectivity)**
Movement Speed	0-50 mph	0-50 knots	0-Mach 2+	0-35K mph+	**Speed of Light, Signal Bandwidth, and Data Throughput Rate**
Forces, Weapons, and Fortifications (Typical examples)	Infantry (Guns, Grenades, Mortars, RPGs), Artillery (Cannons, Rockets, Missiles), Tanks (Guns, Cannons, Rockets), Helicopters (Guns, Rockets, Missiles), Armor, Barricades, Physical Fortifications	Ships, Submarines, Hovercraft, Patrol Craft (Machine Guns, Cannons, Missiles, Rockets, Depth Charges), Armor	Fighters, Bombers, Helicopters (Machine Guns, Cannons, Missiles, Rockets, Bombs), Cruise Missiles, Hardened shelters, Revetments	Satellites, Rockets, Missiles	**All EW Weapons, Malicious Code, EW Jammers, EW Countermeasures, Shielding, Digital Fortifications**

Table 2. Warfighting Domain Attributes Comparison

E. INITIAL OBSERVATIONS

Consolidating the results of the above analysis about the doctrinal attributes of cyberspace with the Warfighting Domain Analytical framework produces Table 2. Based upon these features, additional doctrinal implications can be derived to reveal whether or not the warfighting domain of cyberspace is sufficiently similar to that of the air domain. The interplay between weapons, terrain, fortifications, movement, and maneuver shall be analyzed to determine similarities and differences between the cyber and air domains.

1. Terrain, Operational Movement, and Operational Maneuver

With the continuing proliferation of digital electronics, the WWW, and Internet-enabled devices, much of the digital portion of cyberspace can be visualized as being flat with “oceans” separating physically disconnected networks. Due to the continued proliferation of network technology, bridging these “oceans” between networks is becoming increasingly easy with network bridges, portable storage devices, “sneakernet,”

and the like. The TCP/IP Protocol was originally designed to openly and easily connect as many machines as possible, which tends to flatten cyberspace terrain and make maneuver easy. Mountains or hills do exist in cyberspace in the form of signal bandwidth and data throughput constraints which make traversing certain cyberspace paths more difficult (like climbing uphill). In addition, physical terrain has a direct impact upon the cyberspace domain in the form of signal obstructions and signal attenuation. Additional variations in cyberspace terrain are provided by man-made fortifications. Combined with the fact that cyberspace is constantly growing and expanding, the number of locations from which cyberspace attacks can come from and the number of combinations of network connection options available to aggressors is continuously growing. Also, as TCP/IP technology spreads and connects more electronic devices across the globe, the "oceans" separating networks will continue to shrink. Therefore, digital connectivity across the globe equates to global range. Since digital signals travel at the speed of light, the ability to move and maneuver globally through cyberspace in a matter of seconds enables border and boundary crossings in a matter of seconds. Thus in cyberspace, people (including combatants and non-combatants) can cross sovereign country borders very quickly for operational movement or maneuver. Likewise, fortifications of military installations in cyberspace are only seconds away. Speed and reach are thus the dominant factors in regards to cyberspace attacks and cyberspace power. Under these conditions, the Area of Operations for Computer Network Operations is by definition global. These features make operations in the cyberspace domain more similar to the conduct of operations in the air domain.

2. Man-Made Terrain

Since much of cyberspace is man-made, it is by definition subject to change. As such, the terrain of cyberspace is constantly changing with new hardware and software. This feature allows for creating new cyberspace terrain or destroying it. "Oceans" in cyberspace can be spanned or filled with the introduction of new hardware and/or software. This feature is unique among the other warfighting domains and provides both opportunities and vulnerabilities. The ability to create or destroy cyberspace terrain must be considered a vital component of cyberspace power and thus cyber warfare doctrine.

3. Cyberweapons

Currently, no open source defensive digital weapons currently exist as defined in this paper. That is, no weapons exist that are designed to "shoot down" incoming cyberspace intruders just as Anti-Aircraft Artillery, Surface-to-Air Missiles, or fighter interceptors can shoot down an incoming enemy aircraft. This feature gives attacking forces an advantage, and this feature currently makes the defense of cyberspace more challenging. From the defenders perspective, the defensive options available are 1) to attack the intruders at their home base (an offensive counter cyber mission analogous to offensive counterair mission defined in existing air power doctrine), 2) to "hack back" adversary cyber attacks to determine the source, 3) to absorb enemy weapons effects with fortifications, 4) to move out of the way of the intruders' weapons, 5) to delay intruders, 6) to repair and reconstitute in the event defenses give way, or 7) to implement a combination of these options. These features make operations in the cyberspace domain comparable to that of the air domain. Of course, the advent of true defensive cyberweapons that could shoot down inbound cyber intruders would help to level this playing field considerably.

4. Cyberspace Fortifications and Operational Maneuver

Since no open source defensive digital weapon exist, cyberspace fortifications must currently stand on their own in order to defend a given portion of cyberspace against adversarial attack. However, cyberspace also interconnects various military installations at the speed of light, and these connections result in reducing the maximum strength of all interconnected fortifications to that of the weakest point among them all. In layman's terms, if two castles are connected by an underground tunnel, an attacker only needs to defeat the fortifications of the weaker castle in order to defeat the fortifications of both. Furthermore, defensive maneuvers in cyberspace are typically limited to the friendly system and/or network boundary of the base/enterprise (where defenders have the system administrator or network authority to employ fortifications and operationally maneuver). This is in stark contrast to the attackers vast operational maneuver space. Friendly forces could theoretically counterattack the source of the adversary assault; unfortunately, these countermeasures typically depend upon timely

situational awareness of the cyberspace attack and its source, which typically is not available. Since no defensive digital weapons exist to shoot down incoming attackers, this disparity in maneuverability leans heavily in favor of the attacking force and severely hampers the defense. Finally, defensive maneuvers are severely slowed by insufficient situational awareness, which hinders the ability to plan and execute effective countermeasures. These features are not unlike those associated with the defense of air bases and thus makes defensive operations in cyberspace comparable to defensive operations in the air domain Finally, the development of new methods to enable cyber forces to operationally maneuver across friendly cyberspace would provide friendly forces with the capability to concentrate defensive power against invaders as is doctrinally captured in existing defensive counterair doctrine, thereby making cyber defense even more comparable to air defense.

5. Force Augmentation in Cyberspace

Currently, no reliable methods exist which enable defending forces to operationally move or maneuver along interior lines to concentrate resources to repel incoming attacks at the point of attack. That is, cyber defenders at Base X cannot be readily moved or maneuvered in cyberspace to effectively come to the aid of Base Y that is under attack due to network security policies and limitations across defensive boundaries. As core services continue to centralize and manpower reduced, this has the effect of reducing the overall cyberspace defense capacity of friendly forces.

6. Requirement for Jointness

Of worthy note, these definitions and attributes of the cyberspace warfighting domain do not expose or delineate any significant differences regarding the Army's, Navy's, Air Force's, or Marine's portions of military cyberspace. Cyberspace attacks and cyberspace defense requirements are not unique by or across services. This begs the question as to why each service currently conducts cyberspace operations differently, which creates unnecessary and exploitable seems in operations. Furthermore, these differences can be seen across different Combatant Commands and even within the services themselves. The net effect is the creation and proliferation of unnecessary seams

in the DoD's cyberspace defense operations that adversaries can readily and continually exploit. Therefore, Joint Doctrine for cyberspace operations is vital to unity of effort in the defense of military cyberspace.

F. SUMMARY

By comparing and contrasting the domain of cyberspace to that of the classical warfighting domains of air, land, sea, and space, it is evident that of these four domains cyberspace is most similar to the air domain. Attributes such as the speed of operations, distance of effects, vastness of areas of operations, the permeability of borders/boundaries, degrees of freedom/maneuver, difficulty in building massive fortifications are shared between the air and cyberspace domains. There are also notable differences between the attributes of these two domains that must not be discounted and are worthy of further research. The second closest match is the space domain; however, certain features of the space domain do not lend themselves to useful doctrinal comparison of the cyberspace domain. Namely, the historical record does not provide much material on "space wars" from which to draw historical lessons learned that could be applied to cyber warfare doctrine. For the purposes of this thesis, the warfighting domain of cyberspace is sufficiently similar to that of the air domain to draw credible lessons from the historical development of defensive air power doctrine that can be applied to the development of cyber defense doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

III. BATTLE OF BRITAIN: THE FIRST INTEGRATED AIR DEFENSES

A. HISTORICAL CONTEXT

World War II (WWII) began in the European theater on September 1, 1939, when Germany invaded Poland and incited Great Britain and France to declare war. Between September 1939 and May 1940, Germany had successfully seized control of Denmark and Norway, and by June 1940, the combined military forces of Germany and Italy had successfully seized control of France and effectively driven all remaining British forces off the European mainland. These events set the stage for the Battle of Britain as the first great air battle in history. On one side of the war sat Great Britain alone, and on the other side sat the formidable Germany military. Flanked to the east and south and outnumbered, Great Britain was forced to make a last stand against the oncoming German invasion. Over the course of the next four months (July to October 1940), the Royal Air Force (RAF) successfully defended the skies over the Isles against the formidable German Air Force (Luftwaffe), thereby preventing German military forces from invading their homeland and inspiring Sir Winston Churchill to say, "Never in the field of human conflict was so much owed by so many to so few."[40]

Despite having taken heavy losses over the course of four long months, the RAF was able to successfully defend Great Britain's skies against the Luftwaffe's formidable offensive air campaign by maintaining British air superiority, which thereby limited the damage of Luftwaffe raids and denied the German military of the air cover it desperately needed in order to successfully launch an amphibious invasion across the English Channel. This chapter shall explore how the isolated, outnumbered, and surrounded RAF had effectively employed air power to not only defeat the larger and lethal Luftwaffe but also the entire German war machine attempting to invade England.

[40] "Background to the Battle of Britain," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007.

1. Commander's Intent

In 1940, Hitler's aspirations to invade Great Britain had become increasingly self-evident. Although the particular method and route of the German invasion was the subject of much debate, Sir Winston Churchill anticipated that the Luftwaffe would play a major role in this assault and had charged the RAF with building a fighter and bomber force sufficient enough to "[break] the enemy's attack."[41] Having been driven off the European mainland, British military forces were incapable of launching any major offensive campaign to stave off the coming invasion. For the RAF, this meant that their mission would be to disrupt the Luftwaffe's ability to support or enable the invasion. At best, the RAF would have to maintain air superiority over the Isles, and if they could not, then the RAF would have to deny air superiority to the enemy. Failure to do so would mean that German surface forces would be free to maneuver and launch their air/sea invasion without risk of being struck from the air. It would also mean that the Royal Navy and British ground forces would be at risk of attacks from the Luftwaffe. The major unknown was how long Great Britain's defenses would have to hold against German aggression in order to successfully repel the invasion. In short, a failure to defend British skies would be the prelude to a successful German invasion.

2. Terrain

The geographic situation of Great Britain prior to and during the Battle of Britain was of great concern to British war planners. With German military forces arrayed along the northern coastal regions of mainland Europe just on the other side of the English Channel, most British urban centers and the capital city of London were within striking range of German air power. This fact dictated that the area of responsibility for the RAF would cover all of the British Isles and all possible Luftwaffe approaches. Britain's saving grace was that German ground forces would have to successfully cross the English Channel in order to land sufficient forces to invade and secure England, and during this transition across the Channel, German ground forces would be vulnerable to attack from the Royal Navy and the RAF. Thus, the English Channel served as an effective obstruction to German Blitzkrieg tactics which had been so effective during Germany's

[41]Len Deighton, *Battle of Britain*, 77.

march across Europe. In this situation, Britain also enjoyed the home field advantage and had entrenched its defense forces across the island to fend off any potential German invaders, although equipment, training, and readiness were questionable and problematic. At sea, the Royal Navy was among the best in the world and held a significant advantage over German naval forces, especially after the German Navy suffered heavy losses during previous campaigns. At best, the Royal Navy would enjoy greater freedom of maneuver; at worst, the seas would be contested territory. From the German perspective, Germany had to defeat the Royal Navy as a prelude to landing their ground forces. If the Royal Navy was not neutralized, then their invasion forces on some 3,000 barges and 155 transports would be vulnerable to attacks by the formidable Royal Navy. Since the German Navy was not up to this task after losing half of its destroyers during the Norwegian campaign, the Luftwaffe was called upon to attack the Royal Navy from the air. This fact made the maintenance of British air superiority and the denial of German air superiority all the more critical as a precondition for keeping the German invasion at bay. Lastly, Britain was isolated and surrounded with German forces arrayed from the southwest in France all the way to the northeast in Norway as illustrated in Figure 3. The RAF had to be prepared to repel attacking air forces from many directions.[42]

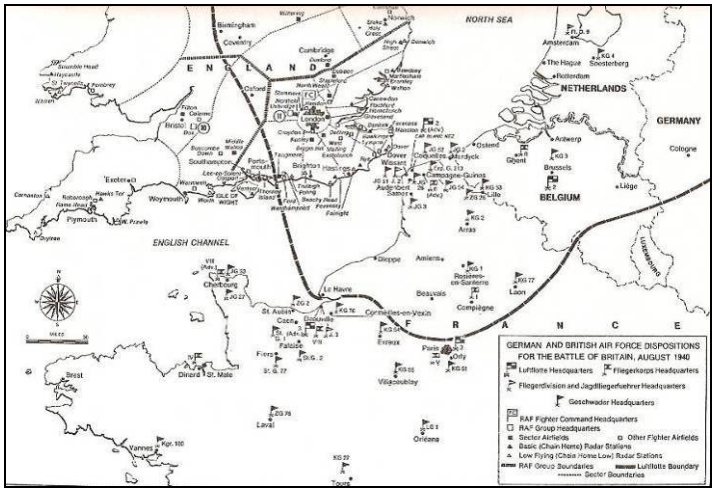


Figure 3. Situation Map: Eve of the Battle of Britain in WWII (From [43])

[42] Len Deighton, *Battle of Britain*, 82-87, 98-99 and Frank W. Heilenday, *The Battle of Britain — Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, Santa Monica, CA: RAND, 1995, 1-2.

[43] Peter Townsend, *Duel of Eagles: The Greatest Book on the Battle of Britain Ever Written*, Edison, NY: Castle Books, 2003, xi.

3. Enemy Forces (Luftwaffe) and Friendly Forces (RAF)

In the summer of 1940, the German military held a significant but not overwhelming advantage in numbers of troops, tanks, and aircraft against the British (see Table 4, Appendix D). The Germans had nearly a 2-to-1 advantage in ground troop strength, nearly a 6-to-1 advantage in tanks (factoring in that only 103 of Britain's tanks were capable of defeating German Panzers), and close to a 3-to-1 advantage in combat aircraft. Whereas the German military forces were well equipped, trained, and supplied, the British military was struggling to recruit, train, and equip sufficient troops for the defense of Britain in such a short time period. Factoring in aircraft serviceability, the Luftwaffe had 824 fighters to Britain's 507 and 1,017 bombers to Britain's meager 84 (see Table 5, Appendix E). The only advantage that the RAF held over the Luftwaffe was that they had more fighter pilots with 1,402 British pilots to Germany's 906 (see Table 6, Appendix E). British and German air forces were arrayed and positioned as illustrated in Figure 4.

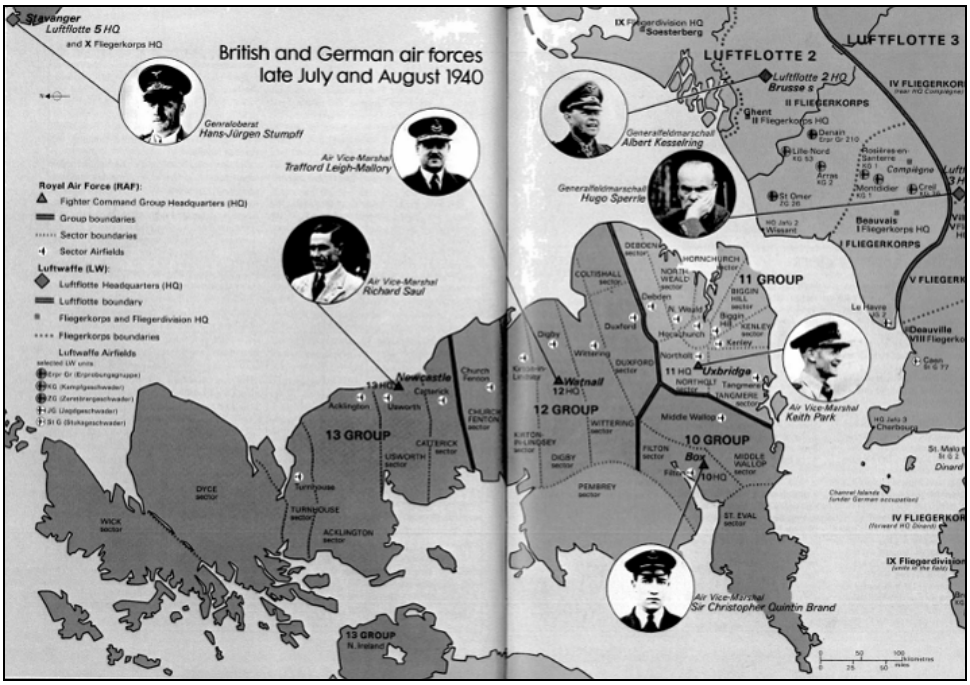


Figure 4. Situation Map: British and German Air Forces (From [44])

[44] Len Deighton, *Battle of Britain*, 98-99.

B. DEFENDING BRITISH SKIES

In analyzing the RAF's defense of Britain, the factors of command and control, operational employment, and technology employment shall be evaluated as they pertained to the United Kingdom's success in the Battle of Britain against the Luftwaffe.

1. Technology Employment

By 1940, the RAF was a very modern and well-equipped air force competing against the equally modern and equipped Luftwaffe. Since World War I and in the run up to WWII, Britain had invested resources in creating a modern air force which included cutting edge fighters, bombers, radar systems, and the defense industrial base needed to support them. Though outnumbered, the RAF would leverage technology to assist them in denying the Luftwaffe air superiority over Britain. A more detailed analysis is required to reveal the factors that contributed to the RAF's success.

a. Aircraft

In 1940, Germany's most advanced fighters were the Messerschmitt Me-109 (officially named the Bayerische Flugzeugwerke or Bf-109) and Me-110; Britain's were the Superman Spitfire and Hawker Hurricane (see Figure 5). The fighters of both nations took advantage of cutting edge technology of the time, but the German Me-109 was arguably the best fighter in the world. Regarding armaments, Luftwaffe fighters held the edge with higher caliber forward guns capable of hitting targets at greater distances. RAF Spitfires and Hurricanes were typically armed only with eight .303-inch guns which had difficulty penetrating armor installed on German fighters and bombers, while Luftwaffe Me-109s and Me-110s were both equipped with two 20 mm cannons which carried more punch and had longer range. In addition, Me-109s carried two 7.92 mm machine guns, and Me-110s carried six 7.92 mm machine guns and a rear gun. Later versions of the Spitfire would eventually be outfitted with two 20 mm cannons to help even the odds. Me-109s and Me-110s also had more powerful engines than their RAF opponents and thus could outclimb and outdive RAF Spitfires and Hurricanes. Me-109s also had fuel injected engines which enabled them to continue operating under negative gravity pushovers; in contrast, the non-fuel-injected British

fighters had to roll over first before diving to avoid starving their engines of fuel. The Me-109 was also outfitted with a supercharger that gave it a decisive performance edge at heights above 20,000 feet against all RAF fighters. The advantage that the RAF fighters had over Luftwaffe fighters was that both the Spitfire and Hurricane were more maneuverable and could turn tighter in a dogfight. The biggest drawback of the Me-109 was its limited range and endurance which provided only about 15 minutes of combat time over southern England despite being forward based near the English Channel. The Me-110's primary drawback was that it was so unmaneuverable that it could not dogfight with British fighters, and its anticipated range and endurance proved disappointing under combat conditions. In summary, the Luftwaffe had an edge in technological capabilities over the RAF going into the Battle of Britain, but this edge was by no means decisive.[45]

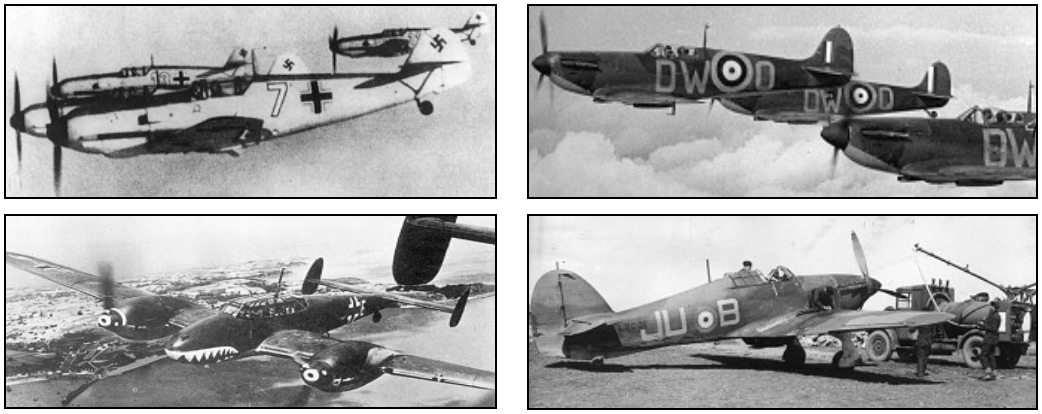


Figure 5. Me-109, Spitfire, Me-110, and Hurricane (From [46])
(top left and right) (bottom left and right)

b. Radar

The Battle of Britain and WWII brought technological changes that would forever transform military defenses by extending human senses beyond their bodily limits in order to anticipate, sense, and thus defeat an adversary at a distance. In the 1930s, both Germany and Britain had experimented with systems that could detect radio waves

[45] Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 3-6; "Aircraft of the Battle of Britain," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007; and Richard Overy, *The Battle of Britain: The Myth and the Reality*, 38-40, 56-60.

[46] "Aircraft of the Battle of Britain," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007.

reflected or re-radiated from distant aircraft. The Brits called their system Radio Detection Finding (RDF), but today we would recognize and call this system radar (RAdio Detection And Ranging). By 1939, German experiments with radar were further along than Britain's; however, Britain was more successful at operationalizing radar to give the RAF improved situational awareness, which they would then translate into tactical and operational successes (see Figure 6). The operationalization of radar included the employment of radar technology combined with the proper mix of operational C2, doctrine, tactics, and training that translated their enhanced situational awareness into combat power on the battlefield.

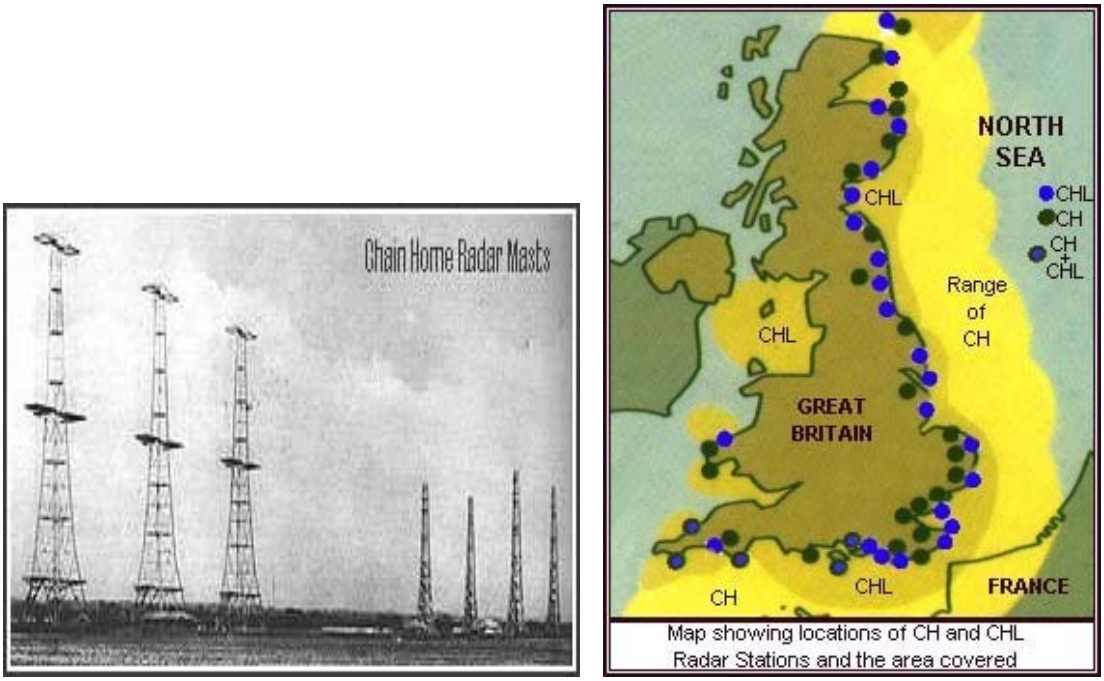


Figure 6. Chain Home Radar Antenna and British Radar Stations (From [47])

Prior to the Battle of Britain, Britain had successfully built and manned 22 "Chain Home" radar stations (each with three 350-foot transmitting antennas and four 240-foot receiving antennas operating at 22-52 MHz radio frequency to detect inbound aircraft as far as 100 miles beyond the coast), 22 "Chain Home Low" radar stations (each with rotating aerial antennas on 185-foot towers operating near 200 MHz to more

[47] "Document 12: The Radar Document," *Battle of Britain Historical Society*, http://www.battlebritain.net, last accessed Feb 10, 2007.

precisely track low-flying aircraft up to 80 miles away as well as ships in the English Channel), and 5 combined radar stations that operated both systems (see Figure 6). Since all British radar systems faced seaward, they could not "see" aircraft after they had crossed the British coastline. These radar stations provided the RAF with near-real-time information on all aircraft approaching the British coast, while the overland radar coverage gap would be filled by the Royal Observer Corps. This wealth of information would require a process and organization that could collect and analyze all radar and observer information, sort out friendly and enemy aircraft, and then communicate with friendly fighters to direct intercepts to enemy aircraft. These issues will be covered in sections B.2 and B.3 of this chapter. This technology, combined with the proper operational C2 and operational employment gave the RAF a significant battlefield advantage in defending the skies over Great Britain.[48]

c. Ground-based Air Defenses

British ground-based air defenses primarily consisted of Anti-Aircraft (AA) guns (see Figure 7). At the beginning of the Battle of Britain, over 130 AA batteries under the Army's Anti-Aircraft Command were positioned to protect vital British centers such as the RAF headquarters, the Rolls-Royce works at Derby, the Bristol aircraft works, Royal Navy bases, key towns, and RAF airfields. AA gun sites were linked to the RAF Fighter Control System which provided AA gunners situational awareness on inbound enemy aircraft and coordinated between airborne defenses (e.g. fighter intercepts) and ground-based defenses (e.g. AA guns). The primary drawback to the AA guns was their lack of mobility which inhibited their ability to be moved in adjustment to changing German tactics and targets. In addition to the AA guns, ground-based air defenses also included a network of 1,466 barrage balloons under the command of the RAF that were tethered around vital targets to discourage low-flying bombers from approaching. These balloons were a deterrent to Luftwaffe pilots, especially at night, but they were also very susceptible to changes in the weather. Alone, these ground-based air

[48] Len Deighton, *Battle of Britain*, 62-63; "The RAF Fighter Control System," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007; and Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 13-15.

defenses stood little chance of countering Luftwaffe attacks or destroying many enemy aircraft. Used in concert with RAF air power, however, ground-based air defenses would add to the battlefield chaos that enemy pilots would have to endure during their attacks.[49]

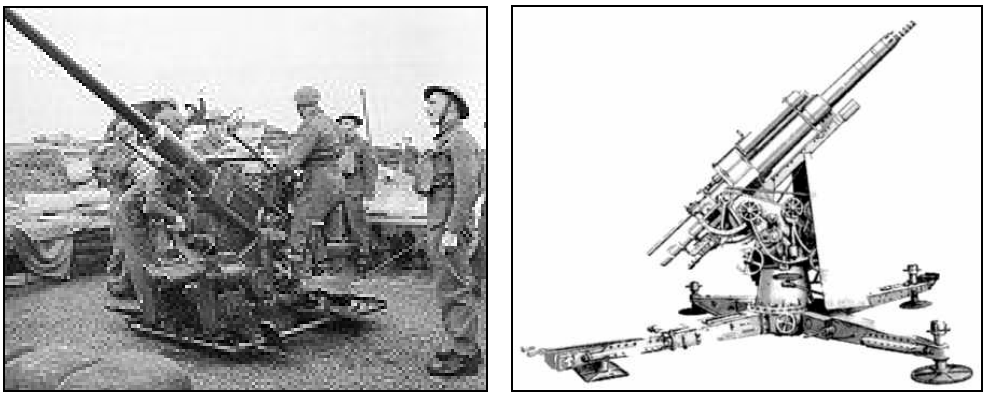


Figure 7. British Anti-Aircraft Gun and Crew (From [50])

d. Military Readiness

Overall, the RAF did a poor job of readying RAF pilots for a long, drawn out air defense campaign. Luftwaffe pilots were typically more skilled in air-to-air engagements, had been superbly trained, and many Luftwaffe pilots were experienced combat veterans from the Poland, France, and Spain campaigns. In contrast, the RAF had sent their best pilots to bomber squadrons during the interwar years, leaving the fighter squadrons to depend upon reservists and the auxiliary for pilot manpower. Thus, British fighter pilots were typically under-trained and none had been formally trained in aerial gunnery. In addition, dated British fighter tactics of flying in tight "Vee" formations were combat ineffective against Luftwaffe fighter tactics, and it was not for several months (and many downed aircraft and pilots) that the RAF would learn and adapt their tactics to match the Luftwaffe. Nevertheless, the RAF sustained several pipelines for recruiting and training pilots to include the RAF College Cranwell, the RAF

[49] Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 7-10 and Len Deighton, *Battle of Britain*, 62-63, 179-185.

[50] "The RAF Fighter Control System," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007 and Len Deighton, *Battle of Britain*, 69.

Volunteer Reserve, and the Halton Apprentices' School. Over the course of the war, successful pilots would share their combat experiences with their peers to improve their tactical proficiency in the air.[51]

RAF ground crews performed remarkably throughout WWII in preparing and repairing combat aircraft for operations. A returning RAF fighter could typically be inspected for damage, refueled, rearmed, and launched within 10-35 minutes while the pilot was being debriefed before the next sortie. Combined with their endurance advantage over Britain (75 minutes combat time for RAF fighters versus 15 minutes for Luftwaffe fighters), this level of sortie generation was critical to multiplying the limited RAF combat aircraft into more combat sorties and thus more combat power. Lastly, by the summer of 1940, Britain had already ramped up its defense industrial base for aircraft production and repair in anticipation of taking heavy losses defending Britain. This industrial mobilization and reconstitution capacity would prove vital to the RAF's capability to sustain a long air defense campaign against the formidable Luftwaffe.[52]

2. Operational Command and Control

Under the leadership of Air Chief Marshal Sir Hugh Dowding and scientific civil servant Henry Tizard, the RAF successfully developed, tested, exercised, and then implemented an integrated air defense system which included radar sites, control centers, airfields, observer stations, and ground-based air defenses across the British Isles.

a. Unified Control and Unified Effort

The fundamental principles of centralized control and decentralized execution laid the foundation of an effective, unified, and coordinated air defense effort. Note that administratively, the various components of military forces defending British skies were assigned under separate chains of command (for example, ground-based air

[51] Len Deighton, *Battle of Britain*, 32-39, 93-94, 110-111 and Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 13, 18-19, 64, 141, 164-165.

[52] Len Deighton, *Battle of Britain*, 32-39, 93-94, 110-111 and Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 13, 18- 19, 64, 141, 164-165.

defenses were under the Army's Anti-Aircraft Command, fighters were under the RAF Fighter Command, bombers were under the RAF Bomber Command, observers were under the Royal Observer Corps, and so forth). Operationally, however, the efforts of these military forces were fused in a simple yet effective operational C2 system called the RAF Fighter Control System (see Figure 8). The RAF Fighter Control System integrated tactical information from across all air defense forces to produce an operational-level common operating picture and shared this "Big Picture" with lower level Group and Sector Control centers which thereby translated this knowledge advantage into the coordinated application of air and ground based defensive combat power.[53]

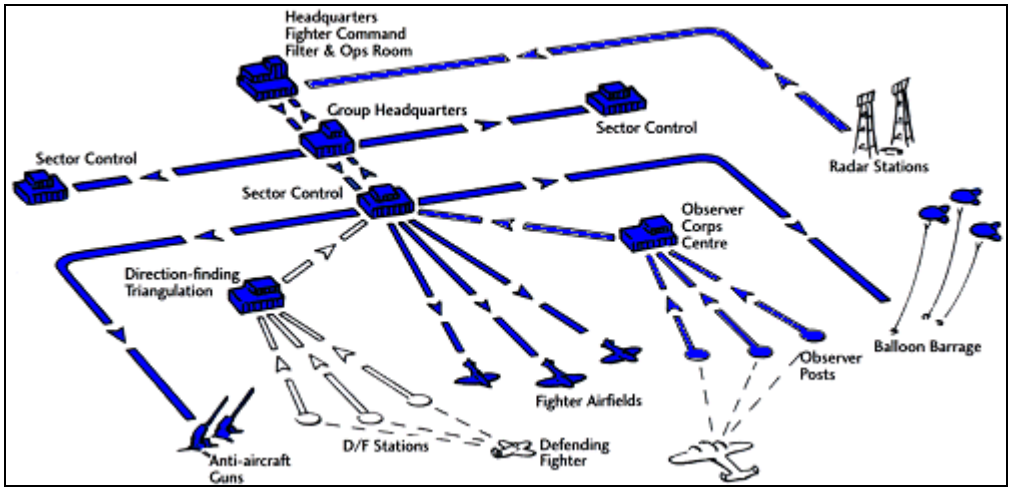


Figure 8. Operational C2 - the RAF Fighter Control System (From [54])

b. Awareness, Centralized Control, and Decentralized Execution

Britain was divided into four regions (see Figure 4), and each region was assigned to a Group Control center. Each group was further subdivided into sectors, and each Sector Control controlled up to three squadrons of fighters, related airfields, AA guns, observer posts, and balloon barrages within that sector. Each Sector Control would pass information (fighter status and enemy aircraft sightings from observation posts) up to Group Control. Group Control would in turn consolidate information from several

[53] British Air Ministry, *The Battle of Britain*, New York, NY: Garden City Publishing Co., 1941, 6-10; "The RAF Fighter Control System," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007; and Len Deighton, *Battle of Britain*, 62-63, 119-120.

[54] "The RAF Fighter Control System," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007.

Sector Controls and would forward this information to Headquarters Fighter Command. All radar reporting (range and bearing of enemy aircraft) was sent directly from all the Chain Home and Chain Home Low radar stations to Headquarters Fighter Command where it was combined with observations (including number, type, heading, and location of enemy aircraft) and to produce a common operational picture (see Figure 9). This "Big Picture" would then be passed back down to Group Controls and Sector Controls, each of which would update their own maps. Sector Controls would then scramble and vector fighters to intercept inbound enemy aircraft, direct AA guns along the inbound aircraft routes, and direct the balloon barrage to launch or adjust as required in preparation for the attack. Each Sector Control would use Direction Finding (DF) radio stations on the ground with Identify-Friend-or-Foe (IFF) transponders aboard friendly aircraft (code named "Parrot") to keep track of friendly and enemy aircraft in order to vector RAF fighters to intercept. Between British radar and ground-observer tracking, Fighter Command could typically vector fighters to within 5 miles and 5,000 feet of the Luftwaffe intruders. Lastly, once RAF fighter pilots visually detected the intruders, they would radio back number, type, position, course, and altitude to Sector Control, which would relay this information to update the common operating picture.[55]

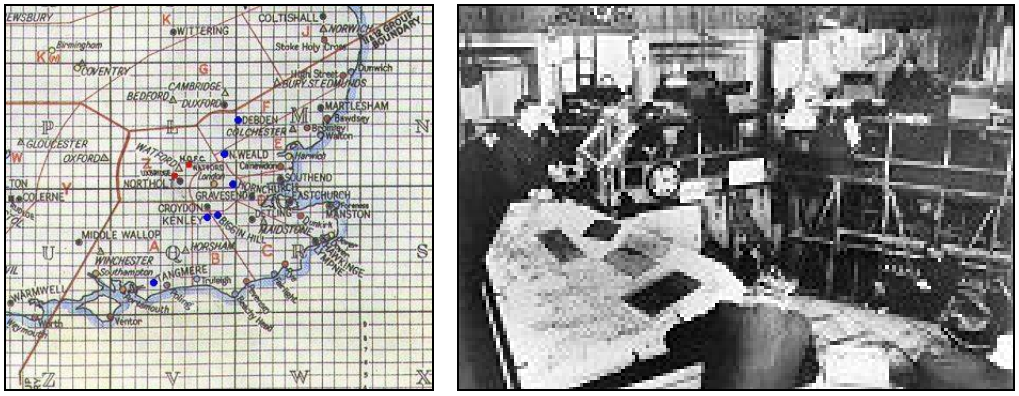


Figure 9. RAF Plot Map and RAF Group Control Center (From [56])

[55] British Air Ministry, *The Battle of Britain*, 6-10; "The RAF Fighter Control System," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007; Len Deighton, *Battle of Britain*, 62-63, 119-120, 179-180; Richard Overy, *The Battle of Britain: The Myth and the Reality*, 42-51; John Monsarrat, "Radar in Retrospect, How It Helped Win the Battle of Britain and the Battle of Okinawa," *Journal of Electronic Defense*, 92-100; and "Document 14: High Frequency Direction Finding," *Battle of Britain Historical Society*, http://www.battleofbritain.net, last accessed Feb 10, 2007.

[56] "The RAF Fighter Control System," *The Battle of Britain History Site*, http://www.raf.mod.uk/bob1940/bobhome.html, last accessed Feb 6, 2007.

c. Operational C2 Summary

The results of this unified operational C2 structure were shared and timely situational awareness and a coordinated air/ground defense. This improved awareness and teamwork significantly contributed to sustaining and drawing out the RAF's air defense campaign despite the technological and numerical edge that the Luftwaffe enjoyed. It would also limit Luftwaffe opportunities to surprise the RAF and enable HQ Fighter Command leaders to make better operational and strategic decisions regarding the air defense campaign of Great Britain.

3. Operational Employment

Although the RAF's C2 structure of centralized operational control and decentralized tactical execution contributed significantly to tactical successes throughout the Battle of Britain, operational doctrine turned this tactical advantage into operational-level leverage.

a. Survivability

In anticipation of a German invasion, the RAF superbly prepared their field forces to survive the inevitable Luftwaffe attacks. Since the objective of the Luftwaffe was to destroy the RAF, RAF survivability became a driving factor to denying the Luftwaffe victory. Using a combination of passive defenses to include camouflage, concealment, hardening (with anti-blast revetments), deception (with realistic dummy airfields and dummy aircraft), interference (with balloon barrage), and dispersal (by scrambling their aircraft once notified of an inbound attack in order to prevent them from being destroyed on the ground), the RAF made the Luftwaffe's task of destroying their RAF combat power much more difficult. Combined with rapid aircraft turnarounds and rapid runway repairs, the RAF could keep their aircraft in the air where their chances for survival greatly improved. In addition, the RAF also kept all less experienced reserve fighter squadrons out of southern England and out of range of the deadly Luftwaffe Me-109s. Active defenses in the form of AA guns made it more difficult for fighters to strafe airfields and would cause Luftwaffe bombers to maneuver to avoid flak and thus reduce the accuracy of German bombs against British targets. Finally, the hierarchical Fighter

Control System provided a measure of C2 redundancy so that the destruction of any given Sector Control center would have a negative impact but would not cripple air defense campaign operations.[57]

b. Operational Maneuver

Since the Luftwaffe did enjoy many tactical advantages in pilot skills, fighter aircraft performance, and sheer numbers, the RAF (Group 11 in particular) struggled for survival during the first month of the Battle of Britain while exacting a heavy cost against the Luftwaffe invaders. Many RAF airfields and aircraft were destroyed and pilots were lost. During this desperate hour, the pressure on Air Chief Marshal Sir Hugh Dowding to either pull the RAF forces back north of the Thames or to throw all of the RAF reserve forces to the north into the fight continued to rise. He resisted because pulling back RAF coverage of southern England would cede air superiority to the Luftwaffe, while throwing all RAF assets into the fight would risk losing them all. Both of these outcomes would result in the Luftwaffe winning the air superiority they needed for the German invasion of England. The RAF only had to deny the Luftwaffe air superiority and had to husband its resources in order to outlast the Luftwaffe; on the other hand, the Luftwaffe would have to destroy and defeat the RAF in order for Germany to prevail.[58]

With their improved situational awareness, RAF Fighter Command was able to employ their limited fighter assets under more favorable battlefield conditions to counter the Luftwaffe's tactical advantages. The Luftwaffe employed deception tactics in an attempt to lure unwitting RAF pilots into air battles advantageous to the Luftwaffe; however, the RAF resisted such engagements and opted instead to wage a war of attrition that would take maximum advantage of Luftwaffe vulnerabilities. For example, Fighter Command would task Hurricane fighters against bombers which did not have Me-109 escorts in order to take advantage of Luftwaffe dive bomber vulnerabilities and stack the odds in favor of RAF fighters. For German bombers that were escorted by Me-109s,

[57] Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 12-13 and Richard Overy, *The Battle of Britain: The Myth and the Reality*, 179-186, and Benjamin Cooling, ed., *Case Studies in the Achievement of Air Superiority*, 140-155.

[58] Peter Townsend, *Duel of Eagles*, 309-326.

Spitfire units would be dispatched instead because they were more capable against and less vulnerable to these German fighters. Furthermore, Spitfire pilots would take advantage of the Me-109's limited endurance by keeping them engaged until they ran out of sufficient fuel to return to their home base. These decisions would accumulate small tactical advantages into larger Luftwaffe aircraft and pilot losses over time and would buy time for the RAF to muster enough strength to challenge the Luftwaffe on the right battlefield. All the while, Britain would continue to produce more aircraft and pilots while protecting its precious combat air forces. Since Luftwaffe intruders could reach coastal targets within twenty minutes of being picked up on radar, Fighter Command used a mixture of three states of alert (Available, Readiness, and Standing by which could take off in twenty, five, and two minutes respectively) to ensure sufficient fighters of the correct type were prepared to intercept the enemy at any given time. RAF doctrinaires that had favored massing RAF fighters to meet the Luftwaffe over southern England had failed to account for the large amount of time it would realistically take to assemble these large air formations, after which any Luftwaffe attack force would already have dropped their ordnance and started heading back to home base. The RAF would have to bide their time until the proper situation presented itself and be cautious to always maintain sufficient reserves to sustain their defenses.[59]

When the Luftwaffe changed their plans from targeting RAF sites (airfields, radar stations, etc.) to bombing London, Fighter Command would make a keen operational adjustment to take advantage of this new opportunity. The geographic proximity of London played a key role in this adjustment for two reasons: 1) London was on the edge of the Me-109's maximum range, and 2) knowing that London was the Luftwaffe's target provided war planners and air controllers sufficient time to assemble large numbers of fighters (from Groups 10, 11, and 12) to meet the incoming air assault in sufficient strength to finally inflict heavy losses. Having preserved a sufficient fighting force, RAF Fighter Command would now choose the right battlefield and conditions in which to employ this force, and that battlefield was the skies over London on September 15, 1940. To meet the first wave of the Luftwaffe attack, the RAF put up

[59] Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 16-18.

17 squadrons (from Groups 11, 10, and 12; about 200 fighters) and held another 12 squadrons in reserve. By operationally maneuvering forces from other sectors to the south, the RAF was able to concentrate sufficient combat power at the right place and time for maximum effect. During this wave, the large RAF formations forced the Luftwaffe formations to breakup, and then British pilots exacted a heavy toll on German fighters and bombers. During the next wave, Fighter Command successfully rallied 26 squadrons (from Groups 11 and 10; about 310 fighters) to meet the airborne invasion force. Using superior situational awareness of the coming attack force, Fighter Command employed operational maneuver between the forces of Groups 10, 11, and 12 to apply sufficient combat power at the right place and time to do the most damage to the Luftwaffe.[60]

c. Operational Employment Summary

By simultaneously coordinating air defense activities over southern England, relocating vulnerable RAF forces beyond the reach of Luftwaffe combat power, and augmenting Group 11 with Group 10 and 12 forces at the right place and time via operational maneuver, the RAF was able to continually delay the Luftwaffe's ability to destroy the RAF. As a result, the RAF was able to deny the Luftwaffe air superiority for an extended period of time (over four months) and thereby prevented Germany's invasion of Great Britain. It is also worth emphasizing the jointness of this operation that often goes unnoticed. One the one hand, Royal Army and RAF forces operated jointly and effectively at the tactical level in the defense of Great Britain's skies; however, Sir Hugh Dowding also clearly understood his joint role in supporting the Royal Navy by denying the Luftwaffe air superiority.

[60] Len Deighton, *Battle of Britain*, 174-178 and Peter Townsend, *Duel of Eagles*, 401-410.

C. OBSERVATIONS AND LESSONS

The RAF was successful during the Battle of Britain because strong leaders like Sir Hugh Dowding were able to weave technology, operational command and control, and an operational doctrine for the employment of air power into a self-reinforcing system that resulted in the effective employment air power.

1. Technological Readiness - Professionalizing the RAF Force

Friendly weapons technology does not have to be the best but must be good enough to defeat the technology of one's adversaries. In addition, weapons technology is only as good as the tactics, training, skills, and experiences of the combat forces employing them. At the beginning of the war, the RAF suffered greatly and unnecessarily by assuming away the need for a viable fighter force in favor of a predominantly bomber force. Over the four months of the Battle of Britain, the RAF eventually adapted their tactics, updated their training, and improved their readiness to the point where RAF fighter pilots could more equitably meet their Luftwaffe counterparts in air battles over England. The need to organize, train, and equip a professional and tactically viable force (to include air and ground crews) is vital to the tactical, operational, and strategic capabilities of the air force.

2. Jointness, Centralized Control, and Decentralized Execution

Every military force has finite resources to employ in combat, and in the art of warfare, these resources must be rallied and employed in the most effective manner to maximize unity of effort and reduce wasted resources and combat power. During the Battle of Britain, the RAF effectively unified the efforts of the joint force (the Army and Air Force) towards the task of defending Britain against the Luftwaffe via centralized control at the operational level. Moreover, at the strategic level, Sir Hugh Dowding's keen insight and acceptance of air power's supporting roll in the joint warfight (namely, the Royal Navy's defense of the English Channel to preclude a German invasion force from landing) often goes unnoticed. Joint unity of effort is critical to maximizing a military's capability to defeat a determined and powerful enemy.

Centralized control of the air defenses of Britain also provided the RAF with the ability to develop holistic, operational-level situational awareness of the airborne battlefield over Britain. With the speed and reach of combat aircraft, a fractured and ground-centric command and control structure would not have enabled any headquarters to acquire a viable common operating picture and then to adjust operations accordingly. In addition, centralized control enabled centralized planning to take advantage of operational-level opportunities when they presented themselves. Since the RAF was not in a position to dictate the operations tempo, Fighter Command instead used this improved situational awareness and centralized control to slow down and draw out the operations tempo to the chagrin of the Luftwaffe battle staff. Centralized control also enabled for the timely updating and dissemination of the common operating picture to all echelons of command and thereby enabled Sector Control centers to make better tactical decisions. Combined with an effective yet primitive radar network, centralized control extended the battlefield awareness of the entire RAF from the Headquarters down to Group Control centers down to Sector Control centers down to the pilots, ground crews, observers, and AA gunners responsible for the decentralized tactical employment of combat power. The speed, reach, and lethality of combat air power dictates that centralized control and decentralized execution is the most effective means of operationally employing defensive air power.

3. Doctrine for Employing Air Power

Many doctrinal principles can be derived from the RAF's historical performance during the Battle of Britain. First, fighting jointly was a doctrinal tenant employed during the Battle of Britain. At the most basic level, the efforts of the Army's Anti-Aircraft Command, the RAF Fighter Command, the RAF Bomber Command, and the Royal Observer Corps had to be unified to support each other in the defense of Britain. A failure to do so would have resulted in the fragmented defense of Great Britain's skies which would likely have allowed the Luftwaffe to gain air superiority.

Second, survivability was another doctrinal tenant used in the defense of Britain. Anticipating potential or real attacks, the RAF prepared their forces to survive. One must assume that in an attack, friendly forces will suffer battle damage and must therefore take

measures to mitigate these effects before, during, and after the attack. Prior to the attack, the use of passive defensive measures such as cover, concealment, camouflage, dispersal, and hardening must be employed to reduce friendly vulnerabilities. During the attacks, the defense force must respond quickly to fend off the attack in order to minimize battle damage and to inflict harm on the opponent. After the attack, forces must have the capacity to quickly repair and reconstitute combat capabilities. From the strategic perspective, the appropriate defense industrial base must be mobilized in order to sustain the military's warfighting capabilities over time.

Third, operational maneuver must be carefully employed in order to maximize friendly advantages and minimize friendly vulnerabilities. Operational maneuver is a necessary part of the response in order to enhance the survivability of friendly forces while inflicting damage upon one's opponents. Operational maneuvers are not limited to merely attacking and defending, but also include moves to relocate, augment, withdraw, and delay. The time and place for particular operational maneuvers is highly dependent upon the current situation. Combined with the improved operational-level situational awareness afforded by the RAF Fighter Control System, Fighter Command was able to operationally defend, relocate, augment, and delay at the right places and times in order to prevent the destruction of the RAF, to buy the time they needed to reconstitute and strengthen their position, and then to concentrate their combat power under more favorable conditions to inflict harm upon and to repel the Luftwaffe invaders.

D. SUMMARY

In summary, the RAF successfully employed defensive air power during the Battle of Britain through the proper combination of operational level command and control, operational employment, and technology employment. As a result, the RAF had superior situational awareness as compared to the Luftwaffe battle staff throughout the entire campaign. Furthermore, this superior awareness enabled the Fighter Command to make more sound operational decisions to prevent the RAF from being destroyed, to slow and draw out the tempo of the campaign, and then to strike with concentrated power when the opportunity presented itself.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SIX DAYS WAR: DISINTEGRATED AIR DEFENSES

A. CONTEXT

On 5 June 1967, Israel launched surprise preemptive air strikes against Egypt to initiate the Six Days War, also known as the June 1967 War. On one side of the war sat Israel alone, and on the other side of the war sat the combined military forces of Egypt, Jordan, and Syria, respectively on the southern, eastern, and northern flanks of Israel.[61] Israel was effectively surrounded on all sides by adversaries and was significantly outnumbered in most aspects. However, after six days of intense fighting, Israel rose as the decisive military victor, leading many historians to characterize this war as how "David conquered Goliath." The Israeli preemptive air strikes served as the spearhead of a surprise, combined arms offensive which enabled the smaller Israeli Defense Forces (IDF) to rapidly and successfully overwhelm the much larger combined Egyptian, Syrian, and Jordanian military forces to decisively seize control of the Sinai Peninsula, West Bank, Gaza Strip, Golan Heights and eastern Jerusalem in just six days.[62] In the words of the militarily defeated King Hussein of Jordan:

> The battle was waged against us almost exclusively from the air with overwhelming strength and continual, sustained air attacks on every single unit of our armed forces, day and night.[63]

Had the Egyptian, Syrian, and/or Jordanian air forces been able to successfully defend against the Israeli offensive air campaign to maintain air superiority (or at a minimum deny air superiority to the Israelis), the outcome of this war would likely have been different. It is arguable whether the Arab states would have prevailed; however, it is reasonable to postulate that a more effective air defense campaign would have enabled Egypt and the Arab states to protect their respective ground forces and to inflict heavy losses on the IAF and IDF. This chapter shall explore how a numerically and arguably

---

[61] Egypt, Syria, and Jordan were the major Arab nations that participated in the Six Days War. Although Iraq, Saudi Arabia, and Lebanon were involved, they were only minimally involved and did not contribute significantly enough to be considered in this analysis. In particular, they did not contribute significantly to the air campaign.

[62] Hal Kosut, ed., *Israel and the Arabs: The June 1967 War*, New York, NY: Facts on File Publications, 1968, 66-67.

[63] King Hussein bin Talal as quoted in Kenneth Pollack, "Air Power in the Six-Day War," 472.

more technologically capable Egyptian Air Force (EAF) had ineffectively employed air power, which quickly led to the decisive defeat of not only their air forces but of the entire Egyptian military. The current literature on the Six Days War provides a wealth of information regarding how the Israeli Air Force (IAF) succeeded in their offensive air campaign; in contrast, this chapter shall not focus on the factors which contributed to the IAF's success but rather shall focus on the factors that inevitably led to the EAF's failure as a prelude to the failure of the entire Egyptian military. In addition, the case of Egypt was singled out (vice Syria or Jordan) because it had the largest military and air force of these three states and presumably should have been the most capable at repelling the IAF. As such, the air war over Egypt in the Six Days War is the focus of this case study.

1. Commander's Intent

With the recent air and ground clashes between Israeli and Syrian forces in April of 1967, the massing of troops on both sides of the Israeli borders, and Egypt instituting a naval blockade of the Gulf of Aqaba at the Strait of Tiran against Israel, the military forces of both sides of this conflict were poised for war on 4 June 1967.[64] In this historical context, one can reasonably assume that the intent of the Commander of the EAF would be to maintain Egyptian air superiority in order to protect and defend Egyptian military forces (air and ground) from any threat posed by the IAF, as well as being prepared to conduct offensive air operations in support of any potential Egyptian ground offensive into Israeli territory. Specifically, Egyptian air superiority would contribute towards a successful Egyptian military campaign against the IDF.

2. Terrain

In many ways, the geographic situation of Egypt prior to and during the Six Days War was comparable to if not better than that of the United Kingdom in the Battle of Britain (see Figure 10). First, the preponderance of Egyptian urban centers and the capital city were relatively far from Israeli ground and air forces, providing a buffer of space and time. In addition, the Egyptian mainland (west of the Suez Canal) was protected by the water barrier of the Suez Canal and the Gulf of Suez. Second, the terrain

[64] Hal Kosut, 39-65.

of much of the Sinai Peninsula itself is hilly and gets more rugged towards the south, which would hinder the advancement of Israeli military ground forces. Towards the northern coastal region of the Sinai, the terrain is flatter and more traversable. Third, Egypt enjoyed the "home field advantage" and had entrenched a large military force to fend off any potential Israeli incursion.[65] Fourth, Egypt enjoyed a measure of sea superiority over Israel in the Mediterranean Sea, Gulf of Suez, and Gulf of Abaqa (where Egypt had initiated the blockade), because Israel's Navy was antiquated.[66] Thus Egypt enjoyed greater freedom of maneuver in the Mediterranean Sea; at worst, the Mediterranean would be neutral territory. Fifth, Egypt was not surrounded by enemies, whereas Israel was. With Saudi Arabia and Jordan covering the southeastern flank of the Sinai, Egypt only had to worry about an Israeli incursion from one direction; whereas, Israel was being threatened along all its land borders.[67]

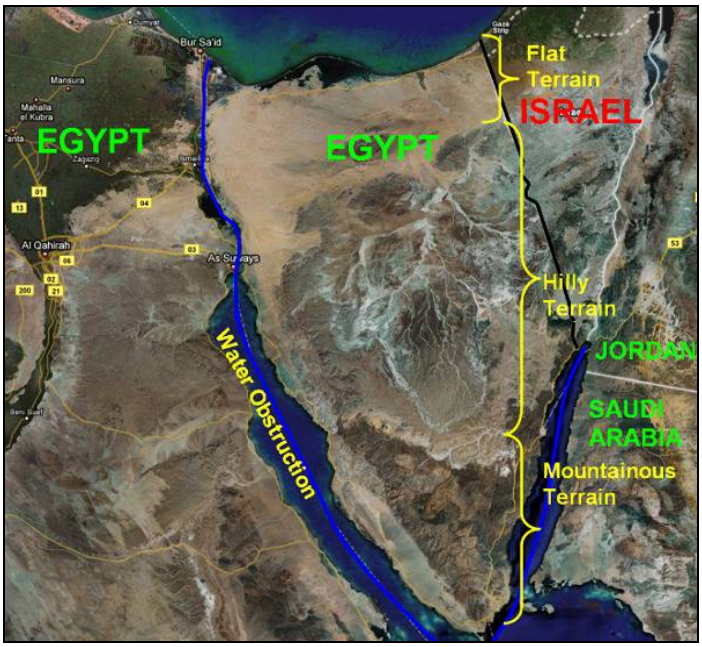


Figure 10. Satellite Image - Sinai Peninsula Terrain (After [68])

[65] Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 60.

[66] "The Israeli Navy Throughout Israel's Wars," *Jewish Virtual Library*, http://www.jewishvirtuallibrary.org/jsource/Society_&_Culture/navywar.html, last accessed Oct 15, 2007.

[67] Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 59.

[68] Underlying satellite image of the Sinai Peninsula provided by Google Maps, http://maps.google.com/maps?f=q&hl=en&geocode=&time=&date=&ttype=&q=egypt&ie=UTF8&ll=29.625996,33.97522&spn=4.048669,6.954346&t=h&z=8&om=1, last accessed Oct 25, 2007.

3. Enemy Forces (IAF) and Friendly Forces (EAF)

On paper, the combined Egyptian, Syrian, and Jordanian forces had Israeli forces outnumbered and outgunned in troops, tanks, and aircraft by a factor of roughly 2-to-1 (see Table 7, Appendix F). In addition, Egypt alone had a nearly 2-to-1 numerical advantage in combat aircraft (especially in fighters) with the EAF bringing approximately 450 combat aircraft to bear against the IAF's 257 combat aircraft (see Table 8, Appendix G). Also, although Egypt could afford to commit most of its air assets to the defense of the Sinai, Israel had to be mindful of the Syrian and Jordanian air forces arrayed to the north and east and thus had to be prepared to use its limited air resources against an additional 127 combat aircraft coming from the opposite direction. Thus the effective combat power of the EAF should have been more than sufficient to maintain Egyptian air superiority over the Sinai Peninsula. Egyptian, Syrian, Jordanian, and Israeli air forces were arrayed and positioned as illustrated in Figure 11.

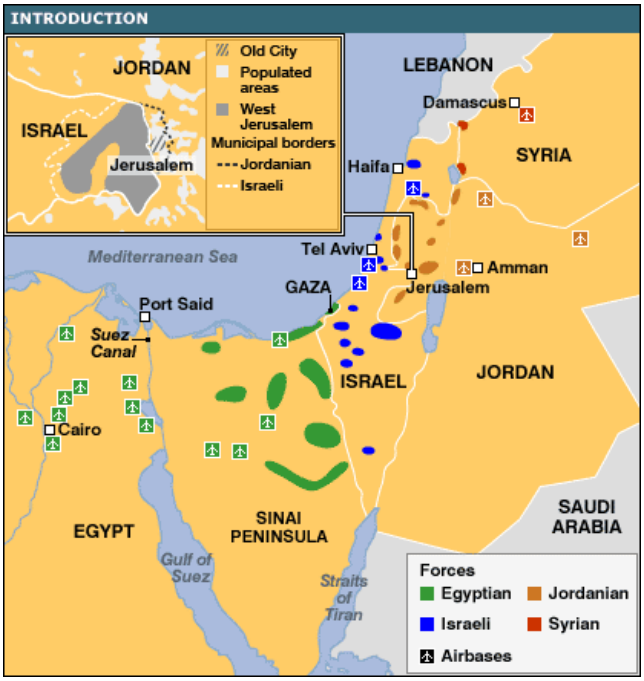


Figure 11. Situation Map: Eve of the Six Days War (From [69])

[69] "1967 Middle East War," *BBC News*, http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457035/html/default.stm, last accessed Oct 25, 2007.

B. DEFENDING EGYPTIAN SKIES

In analyzing the EAF's defense of Egyptian skies, the same factors of command and control, operational employment, and technology employment that were evaluated in Chapter III as they pertained to the United Kingdom's success in the Battle of Britain shall be evaluated as they pertain to the EAF's failure. Conclusions shall be drawn by comparing and contrasting EAF versus RAF performance under comparable conditions.

1. Technology Employment

By 1967, the EAF was a very modern and well-equipped air force and perhaps the most capable air force among all the Arab nations. Egypt had purchased modern radar systems, jet aircraft, armaments, and training from the Soviet Union and had been indoctrinated with corresponding Soviet military doctrine to employ them.[70] Combined with the fact that the EAF enjoyed a significant numerical advantage in raw numbers and in numbers of more advanced weapons and was entrenched on the Sinai, the Egyptian technological edge should have translated into an Egyptian victory. A more detailed analysis is required to reveal the factors that contributed to the EAF's defeat.

a. Aircraft

In 1967, Egypt's most advanced fighter was the Soviet-built MiG-21; Israel's was the French-built Mirage III (see Figure 12).[71] In comparison to the IAF, EAF technology was arguably more advanced, although the IAF's French-built aircraft technology was still very capable. Both aircraft were comparably armed with 30 mm cannons and heat-seeking missiles (the AA-2 Atoll and R.550 Magic respectively), and both aircraft were equipped with airborne radar and a Radar Warning Receiver (RWR) to detect when they were being tracked by ground-based or aircraft-based radar systems.

---

[70] "Arab Air Forces on 5 June 1967," *ACIG Journal*, http://www.acig.org/artman/publish/article_262.shtml, last accessed Oct 15, 2007.

[71] "Arab Air Forces on 5 June 1967" and "5 June 1967 Israeli Air Strikes," *War and Game*, http://warandgame.blogspot.com/2007/10/5-june-1967-israeli-air-strikes.html, last accessed Oct 15, 2007.

Figure 12. EAF MiG-21 and IAF Mirage-III (From [72])
(top) (bottom)

Regarding performance, the MiG-21 held a slight edge since it had more power, a higher maximum speed (1385 mph versus the Mirage's 863 mph), and longer range (721 miles versus the Mirage's 425 miles).[73] In addition, the IAF only had 72 Mirage-IIIs to the EAF's 130 MiG-21s; moreover, the remainder of the IAF inventory included much older systems and technology. In the opinion of the Soviets, Egyptians, and Israelis, the EAF had more than sufficient numbers of Soviet-built fighters to match and/or exceed in quality, capability, and quantity every fighter that the IAF had in its inventory.[74] While both air forces owned fighter-bombers, Egypt also owned and operated the Il-28 light bomber and the Tu-16 supersonic medium bomber. From a technical capabilities perspective, the EAF should have been able to go head-to-head with the IAF.

b. Ground Based Air Defenses

Egyptian ground-based air defenses consisted predominantly of Soviet-built Anti-Aircraft Artillery (AAA) systems and Surface-to-Air Missile (SAM) systems tied to target acquisition, fire control, and target tracking radar systems. These systems were linked into a Soviet-style centralized air defense system to provide operational-level situational awareness of the air defense situation over Egypt.[75] The foundation of the

[72] "Arab Air Forces on 5 June 1967."

[73] "MiG-21 Specifications" and "Mirage III Specification" from *FAS Military Network*, http://www.fas.org and *Combat Aircraft.com*, http://www.combataircraft.com, last accessed Oct 15, 2007.

[74] Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 59-60.

[75] "Arab Air Forces on 5 June 1967."

Egyptian ground-based air defense system was the Soviet-built SA-2 (see left image, Figure 13). The SA-2 system had proven to be a very capable air defense system, for this was the same system that had been used to shoot down U.S. Air Force pilot Francis Gary Powers in a U-2 over the Soviet Union in 1960. On the other side, Israeli ground-based air defense systems were comprised of predominantly French-built AAA systems and the recently acquired U.S.-built HAWK SAM system (see right image, Figure 13) which had been recently added to their weapons inventory in 1965.[76] Both systems were very capable and lethal, but the SA-2 had greater missile speed (Mach 4 versus the HAWK's Mach 2), greater range (40 km versus the HAWK's 24km), and a higher maximum altitude (85,000 feet versus the HAWK's 60,000 feet).[77] Another difference was that the SA-2 was command guided (e.g. remote controlled by its operator) to the target while the HAWK used semi-active radar homing (e.g. ground-based target tracking radar would illuminate the target with radar and the missile would follow the reflected energy back to said target). From a pure technological capabilities perspective, Egyptian ground-based air defense systems should have been capable of inflicting heavy losses against the IAF.

Figure 13. Egyptian SA-2 and Israeli HAWK Surface-to-Air Missiles (From [78])
(left) (right)

[76] "HAWK," *Israeli Weapons.com*; "5 June 1967 Israeli Air Strikes;" "HAWK Missile B-7-5: History of the Hawk Missile System," http://www.geocities.com/hawkmissileb75/history.htm?200726, last accessed Oct 25, 2007; and "Operation Moked: Destruction of Arab Air Forces," *ACIG Journal*, http://www.acig.org/artman/publish/article_260.shtml, last accessed Oct 15, 2007.

[77] "SA-2 GUIDELINE," *FAS Military Network*, http://www.fas.org, last accessed Oct 15, 2007 and "HAWK," *FAS Military Network*, http://www.fas.org, last accessed Oct 15, 2007.

[78] "HAWK," *Israeli Weapons.com*, http://www.israeli-weapons.com/weapons/missile_systems/surface_missiles/hawk/Hawk.htm, last accessed Oct 26, 2007 and *Egyptian National Military Museum*, http://www.richard-seaman.com/Aircraft/Museums/EgyptianNationalMilitaryMuseum/index.html, last accessed Oct 26, 2007.

c. Military Readiness

The EAF was well-equipped with numerous state-of-the-art weapon systems against an arguably inferior IAF, and they significantly outnumbered the IAF. Second, Egypt was operating on its home turf, while Israel would have the burden of seizing territory. Given that these factors were stacked in favor of the EAF and yet they were defeated, one more factor must be assessed in order to explain why the EAF suffered so greatly at the hands of the IAF. This last factor is military readiness.

In the simplest terms, technological capability is limited to the skills of the personnel that employ it. Simply having better weapons does not equate to battlefield success unless one's personnel are properly trained to employ them; only then can the technical edge of one's systems be translated into a competitive battlefield advantage. In this regard, the EAF failed miserably to provide the necessary skills to its forces charged with defending Egyptian skies. For example, the EAF as a whole had only a 70 percent operational readiness rate, and the readiness of the EAF's premier MiG-21 squadrons was only 60-65 percent.[79] As such, Egyptian fighter pilots were no match for their IAF counterparts. On the first day of the war, 20 percent of the EAF force was not operational because of the combination of 1) the poor proficiency of ground crews to generate sorties (e.g. repair and prepare aircraft for combat) and 2) the poor skills of pilots to fight in the air. Poor readiness was such a problem that the U.S. Central Intelligence Agency had accurately assessed that the IAF was capable of attaining air supremacy over the Sinai in less than 24 hours if they initiated the offensive or within two to three days if Egypt attacked first.[80] Egyptian ground-based air defense forces faired a little better and thus accounted for the preponderance of downed IAF aircraft, mainly by AAA fire;[81] however, the overall lack of professionalism and readiness turned the IAF's success on the battlefield into the EAF's slaughter.

---

[79] Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 74-76.

[80] "Military Capabilities of Israel and the Arab States," http://www.sixdaywar.co.uk/graphics/arab-israeli_memo.jpg and "Arab-Israel Six Days War: Intelligence Memorandum Prepared in the Central Intelligence Agency, May 26, 1967," http://www.zionism-israel.com/hdoc/CIA_on_War_Estimate_1967.htm, last accessed Oct 25, 2007.

[81] "Arab-Israeli Aircraft Losses," http://www.geocities.com/CapeCanaveral/Hangar/2848/losses.htm, last accessed Oct 25, 2007.

2. Command and Control

Between 1956 and 1967, Egyptian national and military decision makers had reorganized the EAF in alliance with Soviet ground-centric military doctrine. At the top of the EAF organizational structure sat the General Headquarters (GHQ), under which sat the Supreme Command Council (SCC). Below the SCC, air forces were organized into Air Brigades of three Squadrons each of which were tied into a centralized air defense system controlled by the SCC. Despite most Air Brigades being organized under the centralized control of the SCC, several Air Brigades were also put under the direct control of the Army under the respective ground commander's local control centers. In fact, several Squadrons that were supposed to be under the control of the SCC via their respective Air Brigade were also chopped to localized Army control. Local control centers were integrated into a Soviet-style command and control system and were supported by 12 radar stations and ground observers. Figure 14 provides an illustration of the operational C2 structure of the EAF during the Six Days War. In addition, the command-and-control of the aforementioned ground-based air defense forces (AAA and SA-2 SAMs) was comparably dispersed amongst commanders in the field according to geography.[82] Several conclusions can be drawn about this convoluted EAF C2 structure.

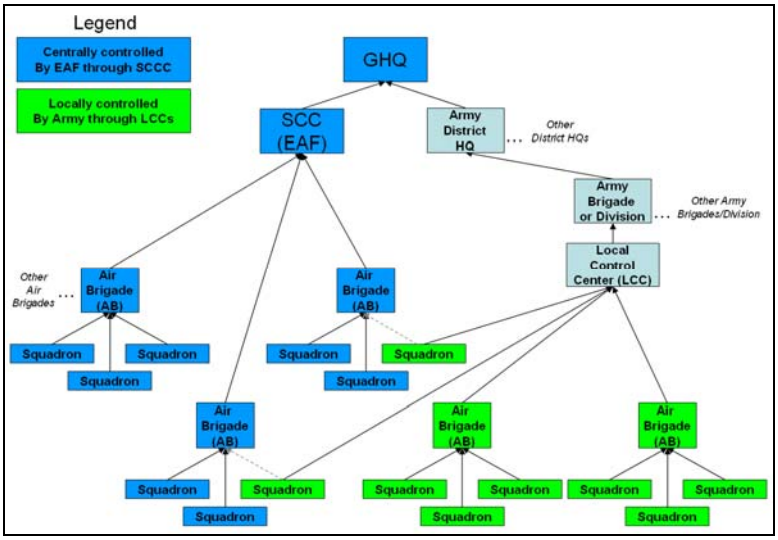


Figure 14. Operational C2 of the EAF

[82] "Arab Air Forces on 5 June 1967."

a. Fragmented Unity of Effort

First, two separate entities were responsible for the air defense of Egypt: the EAF and the ground-based air defenses (some under Army and others under EAF control). However, these two lines of effort were never unified. Referring to Figure 14, no one had been clearly designated as responsible for the air defense of Egypt. This factor became most evident when Egypt had to shut down its own air defense systems on the first day of the war for fear that Egyptian AAA and/or SA-2s might inadvertently shoot down the air transport carrying Field Marshall Abdel Hakim 'Amr (Commander of the Egyptian Armed Forces) and Lt Gen Mahmud Sidqi Mahmud (Commander of the EAF) on board.[83] The result was that no one was designated overall in charge of the air defense of Egypt, and no one took the initiative to take charge. If an entity was actually in charge of the unified air defense of Egypt, one would expect to find evidence of this central air defense authority in the form of a unified air defense plan or orders to coordinate the actions of EAF field units and/or ground-based air defense units; however, no such plans or orders can be found in the historical record. This disunity of effort was not only internal, but was also external. After Egypt had coaxed Syria and Jordan to join the war, no one unified the efforts of the collective Egyptian, Syrian, and Jordanian air forces and air defenses. As a result, the air defense of Egypt was fractured both internally between the EAF and ground-based air defenses, between EAF units themselves, and across the combined air forces of the EAF, Syrian Air Force, and Jordanian Air Force.

b. No Control and Centralized Execution

Second, the EAF command enforced highly centralized control and centralized execution, having concentrated all authority at the top and delegating none to lower level commanders. As a result, the EAF as a whole was very slow to respond on the battlefield because field commanders would wait for their orders before taking any action. The net result was that EAF officers at all levels literally froze until they received orders from their higher headquarters. This would include Egyptian air bases that refused to launch aircraft that had survived the initial IAF attack wave without orders to do so

[83] Jeremy Bowen, *Six Days: How the 1967 War Shaped the Middle East*, New York, NY: Thomas Dunne Books, 2005, 114-115 and Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 63.

from above. As a result, many of these aircraft were destroyed on the ground in successive IAF attack waves. This effect was further exacerbated when Lt Gen Mahmud Sidqi Mahmud (Commander of the EAF) found himself stuck on an air transport in the air in search of an undamaged airfield on which to land. Since he was effectively out of the fight and all EAF operational and tactical authorities were held in him, the head of the EAF war machine had effectively been chopped off paralyzing the entire EAF. In addition, this centralized control and centralized execution further hindered cooperation between the EAF and the Egyptian Army and Navy, resulting in poor joint support and performance.[84] Throughout the entire war, centralized control and centralized execution effectively and efficiently paralyzed the EAF at all command levels and prevented them from organizing their 140 remaining fighters to defend Egyptian airspace.

c. No Situational Awareness

Operational level situational awareness of the air defense of Egypt was severely hindered due to the matrixed chain of command. At no point in this organizational structure does the complete air picture over Egypt ever accumulate to provide any commander sufficient awareness of what was happening on the battlefield over the Sinai or mainland Egypt. Though the centralized air defense system attached to the SCC was supposed to provide centralized control of all air defenses, there is no historical evidence that SCC personnel were aware of what was really happening or that reports from the field were being channeled to the SCC to provide accurate updates. This factor would be further exacerbated by lies told by military officers at all levels in an attempt to cover up how much damage had been done to the EAF on the first day of the strikes, to include lies told by Field Marshall ‘Amr to President Nasser to cover up the fact that a large portion of the EAF had been destroyed. There is also evidence in the form of contradictory reporting from all levels of the Egyptian chain of command that no one in the EAF knew what was happening.[85] The fractured organizational structure contributed to piecemeal situational awareness which crippled the EAF.

---

[84] “Arab Air Forces on 5 June 1967” and Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 62-64 and 74-76.

[85] Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 69-71.

d. C2 Summary

The end result of the EAF's fractured organizational structure, centralized control and centralized execution, and fractured situational awareness turned what should have been the modern integrated air defenses of Egypt into disintegrated air defenses, which the IAF exploited and destroyed. There was no unity of effort exhibited by the EAF during the entire Egyptian air defense campaign. These factors combined with the poor readiness of EAF forces with disastrous and lethal results.

3. Operational Employment

EAF forces and aircraft were positioned at 25 main bases supported by ground-based air defense systems.[86] Besides the aforementioned problems with technology employment and command and control, the EAF further exacerbated their failed performance with the poor operational employment of their air defenses, both air and ground-based. In this venue, the EAF failed on two fronts: 1) they failed to adequately prepare for attack, and 2) they failed to effectively regroup and respond to the attack.

a. Survivability

On 4 June 1967, the EAF was completely unprepared for war against the IAF. Regardless of the contradictory reports coming from Egyptian intelligence as to whether Israel would attack, the Egyptian military and EAF leadership should have anticipated that war with Israel was possible and made the necessary preparations for such an event. The only two options in the event of war would be either Egypt would attack first or Israel would attack first. Since President Nasser did not anticipate that Egypt would launch an attack,[87] Egyptian military leaders should have anticipated that in the event of war, Israel would likely initiate aggression. As such, they should have been prepared for just such as event; however, they were not, as was evident by their many inactions. Blind to their own vulnerabilities, the EAF was effectively postured for destruction by the IAF. First, the entire EAF was not prepared to be struck. Specifically,

[86] John F. Kreis, *Air Warfare and Air Base Air Defense, 1914-1973*, Washington, DC: Office of Air Force History, U.S. Air Force, 1988, 307-316.

[87] Ronald E. Bergquist, *The Role of Airpower in the Iran-Iraq War*, Maxwell AFB, AL: Air University Press, 1988, 7.

EAF aircraft were lined up neatly in rows on their respective airfields, which made IAF targeting and destruction all the more easy.[88] No efforts to conceal, harden, or disperse valuable EAF air assets were conducted at any of the 25 bases, and camouflage efforts with the placement of dummy aircraft had limited effectiveness.[89] This was akin to the situation the U.S. Navy faced when it lined up all of its warships to make them easier for the military police to guard just prior to the Japanese attack on Pearl Harbor. In addition, the EAF was not on alert on 5 June 1967, although they had been on alert just two days prior. Lastly, EAF military leaders did not know what an IAF attack might look like and did not bother to ask said question. As such, EAF war planners did not recognize that air bases in the Sinai Peninsula and those located in proximity to Egyptian urban centers along the Nile were well within striking range of IAF aircraft. Simple math reveals that IAF aircraft could strike targets in mainland Egypt in less than 1 hour. Yet EAF forces were not postured accordingly, as was evident when most of their aircraft were destroyed on the ground after returning from their morning patrols while many EAF officers were still on their way to work. Finally, EAF field commanders had no standing orders, authorities, or procedures as to what they should do in the event of an attack. These failures in operational leadership combined with poor military readiness and a micromanaged yet fractured command and control structure inevitably contributed to the destruction of 18 Egyptian air bases and the loss of some 300 EAF aircraft and 100 pilots.[90]

b. Operational Maneuver

Even though the first day of IAF attacks dealt a devastating blow to the EAF, the EAF still had approximately 140 fighters that could have been mustered to defend the skies over Egypt; yet this operational level response never occurred. In addition, the Syrian and Jordanian air forces could have brought another 121 fighters to bear. Yet, the EAF as a whole failed to regroup and then to organize a coordinated

---

[88] John Kreis, *Air Warfare and Air Base Air Defense, 1914-1973*, 316.

[89] Ronald Bergquist, *The Role of Airpower in the Iran-Iraq War*, 8.

[90] Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 62-63 and Major Charles B. Long, "Analysis of the Six Days War, June 1967," *Air Command and Staff College Distance Learning CD Version 3.2*, Maxwell AFB, AL: Air University, 2003.

response to IAF aggression. Despite 18 air bases being struck, dedicated runway repair crews were able to repair most runways quickly.[91] With over 250 fighters still available between the EAF, Syrian Air Force, and Jordanian Air Force to meet the IAF, the EAF failed to coordinate a unified response that could have massed sufficient resources and maneuvered them into a more effective defense against the IAF. The EAF lacked a theory of air power doctrine, and thus no plan was ever developed and little to no coordination was done to maneuver or concentrate the remaining air force assets for maximum effectiveness.[92] No effort was made to unify the effects of ground-based and air defenses. Coordination with the Syrian and Jordanian Air Forces was minimal at best. The net result was a very static and fragmented air defense campaign. The remaining EAF pilots and aircraft bravely took to the skies to do battle with the IAF in poorly coordinated and dispersed waves, only to return with fewer aircraft.[93]

c. Operational Employment Summary

The EAF's piecemeal application of air power enabled the IAF to concentrate its forces against adversaries in a sequential fashion so as to never be outnumbered while the Arab air forces had effectively divided themselves to be conquered. A coordinated EAF air campaign could have created sufficient space and time for Egyptian ground forces on the Sinai Peninsula to safely retreat without being massacred, and at best, such a coordinated effort might have inflicted heavier Israeli losses and drawn out the length of this campaign to change the outcome of the entire war.

C. OBSERVATIONS AND LESSONS

The EAF clearly failed during the Six Days War because Egyptian military leaders had not properly integrated technology, operational command and control, and an operational doctrine into effective combat air power.

---

[91] Benjamin F. Cooling, ed., *Case Studies in the Achievement of Air Superiority*, Washington, DC: Air Force History & Museums Program, 1994, 578.

[92] Robin Higham, "The Arab Air Forces" in Robin Higham and Stephen J. Harris, eds., *Why Air Forces Fail: The Anatomy of Defeat*, 78-80.

[93] Ronald Bergquist, *The Role of Airpower in the Iran-Iraq War*, 7-9; Kenneth Pollack, *Arabs at War: Military Effectiveness, 1948-1991*, 62-64, 74-76, and 84-88; Kenneth Pollack, "Air Power in the Six-Day War," 488-489; and "Arab Air Forces on 5 June 1967."

1. Failure of Technological Readiness - The Unprofessional EAF

Although EAF weapons technology was superior in quality and numbers to that of the IAF, the EAF failed to integrate the most important component of these weapon systems--people. Weapons technology is only as good as the tactics, training, skills, and experiences invested in the combat forces employing them. At the outset of the war, the EAF suffered tremendously by failing to train enough fighter pilots to fight against their IAF adversary. This mission readiness was also reflected in poor ground crew readiness and the poor aircraft serviceability and turnaround rate that resulted. Over six days, EAF pilots climbed into the air only to be shot down by the lethal tactical prowess of their IAF counterparts. Unfortunately, the Egyptians did not have four months to regroup and retrain their pilots like the RAF did during the Battle of Britain. The need to organize, train, and equip a professional and tactically viable force (to include air and ground crews) is vital to the tactical, operational, and strategic capabilities of the air force.

2. Fragmented C2 Equals Operational Paralysis

The EAF also failed to unify the efforts of the joint force or even their own air forces to defend Egyptian skies. On paper, the Soviet-style centralized air defense system was supposed to integrate air based (e.g. fighters) and ground based air defenses (e.g. AAA and SAMs); however in implementation, some EAF squadrons fell under the operational control of the Army while the majority of the EAF forces remained under SCC control. Also, ground-based air defense forces were under the operational control of Army commanders. The operational command and control structure was dictated by the varying service cultures and demographics instead of being dictated by the mission at hand, which was to defend Egyptian aerial territory. Therefore, no one entity was in operational control of or responsible for all Egyptian air defenses.

Due to the highly centralized command structure and culture of the EAF and the Egyptian military in general, most EAF units refused to launch their fighters without explicit orders. Since no one was operationally in charge of all Egyptian air defenses, no operational level plan was developed for the air defense of Egypt and related tasks and orders could not be disseminated to EAF units. All EAF units could do was to launch responsively in ineffective attempts to fend off the IAF intruders. This failure to unify

the joint air defenses of Egypt, to centrally control and centrally plan for said air defense campaign, and to decentralize tactical execution culminated in operational level paralysis of all Egyptian air defenses. Finally, the most telling evidence supporting this effect is that the IAF did not specifically target major EAF command and control nodes; instead, they targeted EAF fighter and bomber forces on the ground. Yet the EAF was still operationally paralyzed.

3. No Doctrine for Employing Air Power

Although the EAF failed to defend Egypt during the Six Days War, many doctrinal principles can still be derived from their failed performance. First, the EAF failed to fight jointly and thus failed to unify the efforts of their AAA and SAM forces in the Army and of their own EAF forces. The result was a clearly fragmented response in the face of skilled and lethal IAF aggression. The IAF took clear advantage of this seam to quickly and decisively seize air superiority over Egypt.

Second, the EAF never properly considered survivability. The EAF had not anticipating potential or real attacks from the IAF and therefore failed to prepare their forces to survive a surprise attack. One must reasonably assume that during an attack, friendly forces will suffer battle damage, and military leaders must therefore take measures to mitigate these effects before, during, and after attacks. Instead, the EAF parked their aircraft in neat rows which made the IAF surprise attack all the more destructive. Prior to the attack, passive defensive measures such as cover, concealment, camouflage, dispersal, and hardening were not employed to reduce friendly vulnerabilities. Feeble attempts at unrealistic deception were the only indication of any anticipatory EAF preparations. During the attacks, defense forces could not respond quickly enough to fend off attackers. After the attacks, the EAF did not have sufficient capacity to quickly repair and reconstitute their combat capabilities. The IAF fully exploited the EAF's failure to plan for survivability with devastating results.

Third, the EAF failed to employ any operational maneuver in their impotent attempt to drive back the IAF. The remaining EAF forces were launched in a haphazard fashion which did not take into consideration minimizing friendly vulnerabilities and

maximizing opportunities. The Egyptian defensive posture remained very static, which made the mission of the IAF much easier. Fighters were not on alert in the event of an IAF attack. Precious fighter resources were never sufficiently concentrated at the right places and times to have any effect. For example, Egyptian, Syrian, and Jordanian air efforts were not coordinated and integrated, which thereby allowed the smaller IAF to take on and defeat each enemy in turn instead of facing a multi-front threat. As another example, a continuous wave of moderately sized air formations employing hit and run tactics could have be used to constantly harass the IAF throughout the campaign. Although the EAF was not tactically proficient enough to challenge IAF pilots in a fair fight, these harassing hit and run tactics may have challenged Israeli air superiority enough to buy time and space for the Egyptian ground forces to retreat without being massacred. The EAF did not husband their remaining IAF combat forces for a sustained and drawn out conflict and did not make the operational level adjustments necessary to challenge Israeli air superiority.

D. SUMMARY

In summary, the EAF failed miserably to employ defensive air power during the Six Days War. Their failure to properly combine operational level command and control, air power doctrine, and technology gave the IAF a decisive advantage over the EAF. The inevitable results were the loss of Egyptian air superiority followed by the routing of Egyptian ground and air forces and the loss of the war.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INTEGRATED CYBER DEFENSES: PREPARING FOR THE FIRST REAL CYBERWAR

A. BUILDING AN INTEGRATED CYBER DEFENSE

Many nation-states have recognized the untapped strategic and operational opportunities and vulnerabilities associated with cyber warfare and have thus invested significant resources towards the development of their respective cyber warfare capabilities.[94] In response to this emerging threat to U.S. national security, the DoD must not only develop offensive cyber warfare capabilities but must also develop the respective defensive cyber warfare capabilities in anticipation that U.S. adversaries will likely employ cyberweapons against U.S. military forces. Although defensive capabilities cannot win a war, a failure to develop viable defenses can lose a war. By combining the observations from Chapters II, III, and IV, this chapter shall recommend that the DoD invest resources towards the development of integrated cyber defense capabilities analogous to historically successful integrated air defenses. These recommendations shall contribute to filling the current doctrinal gap regarding Computer Network Defense and will include recommendations regarding technology employment, operational employment, and operational command and control.

On a clarifying note, integrated cyber defenses are not to be confused with an Integrated Cyber Defense System, just as integrated air defenses are not to be confused with an Integrated Air Defense System. Integrated air defenses and integrated cyber defenses are holistic capabilities; whereas, Integrated Air Defense Systems and Integrated Cyber Defense Systems are systems designed to provide these capabilities. From Chapter III, one can surmise that the RAF had successfully developed and employed integrated air defense capabilities during the Battle of Britain. In contrast in Chapter IV, it is clear that although Egypt had purchased an Integrated Air Defense System from the Soviet Union, they did not develop or employ effective integrated air defense capabilities during the Six Days War.

---

[94] Charles Billo and Welton Chang, *Cyberwarfare: An Analysis of Means and Motivations of Selected Nation States*, 2004.

B. THOUGHT EXPERIMENT - THE FIRST REAL CYBERWAR

Italian airpower theorist Giulio Douhet wisely stated that "Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur." In keeping with this theme, this chapter shall use a thought experiment about what the first real cyberwar might look like to help illustrate the integrated cyber defense capabilities that the DoD needs to develop. This thought experiment shall make several reasonable assumptions regarding the nature of this war based upon analogous lessons drawn from the case studies in Chapters III and IV. The opposing forces for this thought experiment shall be the United States and a peer competitor state with comparable warfighting capabilities in the air, land, sea, space, and cyberspace domains. To better illustrate the defensive capabilities required, the peer competitor state shall initiate aggression in this conflict, just as Britain's and Egypt's respective adversaries had done in the two cases studied. We shall also assume that this adversary shall employ their air, land, sea, space, and cyberspace forces in a coordinated, combined arms fashion to maximize their asymmetric battlefield advantages and to exploit U.S. military vulnerabilities. As such, the DoD would have to mount an effective defense across all warfighting domains in the face of this aggression. More specifically, this chapter shall explore the DoD integrated cyber defense capabilities needed in order to defend DoD cyberspace. Since this war will occur some time in the future, assume that both opponents possess more powerful cyber weapons than are in existence today (beyond mere web defacements, denial of service, information thefts, etc.). Thus, the ability of U.S. military forces to fight would depend in large measure upon its ability to defend the computers and networks upon which the DoD has become so dependent.

1. Technology Employment

Prior to this cyberwar, the DoD needs to invest in several technologies to provide the foundational tactical capabilities needed to defend friendly cyberspace. Using the RAF's effective example of technology employment as a model, the DoD should develop a Cyber Sensor Net (comparable to the RAF Radar Network), Cyber Identify-Friend-or-Foe (Cyber IFF; comparable to aircraft IFF), and defensive weapons (comparable to AAA, SAMs, or fighter interceptors).

a. Cyber Sensor Network

Just as the RAF Radar Network had pushed the RAF's situational awareness about Luftwaffe intruders beyond 100 miles beyond their borders, a comparable Cyber Sensor Net should be built to push DoD cyber situational awareness beyond U.S. borders. Leveraging the attributes of the domain of cyberspace (see Chapter II), it seems reasonable to assume that such a system is technically feasible. This is in contrast with current industry computer and network security methods that focus heavily upon the fielding of internal sensors such as intrusion detection systems, firewalls, anti-virus scanners and so forth that detect attacks after they've hit or passed friendly network perimeters. This Cyber Sensor Network must be pushed outwards to provide the DoD with the situational awareness needed to see an inbound attack in progress instead of waiting for the attack. The deployment of this sensor network should include posting sensors outside DoD networks through partnerships with the private sector, allied governments, and or covert operations. One can reasonably assume that a determined peer competitor is already developing this type of sensor capability. Furthermore, the further out this Cyber Sensor Network can see, the better, since cyber attacks can occur at the speed of light. Due to this speed, this Cyber Sensor Net may provide the first indications of not only the inbound cyber assault but also of the corresponding and pending attacks in the other four warfighting domains. Finally, existing internal sensors must also be integrated to provide a common operating picture of the cyberspace battlefield to include friendly and enemy territory.

b. Cyber Identify-Friend-or-Foe (Cyber IFF)

Current network security systems focus on trying to sort out adversarial cyber activities from the vast amounts of data being stored, processed, and exchanged, and cyber attackers use this to their advantage by purposefully hiding in the vastness of cyberspace. Technology also needs to provide a means by which to clearly identify friendly forces as well as adversaries in cyberspace. In this venue, current initiatives such as the enterprise-wide deployment of Public Key Infrastructure fulfills part of this requirement. However, cyberspace also includes friendly systems and software that could be clearly flagged and identified to limit the scope of the search for cyber intruders.

A variety of technologies already exists today (application checksums, digital signatures, Microsoft Group Policies, and so forth) but have not been integrated into a holistic cyber IFF system. Today, various intrusion or malicious logic scanners must typically scan every file on every system or every packet. In large measure, cyber defenders today do not have a comprehensive method by which to identify "bandits" (adversaries) versus friendlies versus "bogies" (unidentified). Thus, almost all DoD cyberspace falls into the "bogie" category, making the identification of bandits more problematic and the potential for "cyber fratricide" greater. A Cyber IFF capability could reduce this searching to better concentrate limited resources towards the task of finding adversaries.

c. Defensive Cyber Weapons

As mentioned in Chapter II, no open source defensive digital weapons currently exist that can shoot down inbound intruders. The only options currently available to fend off a cyber attack are to attack the target at its source, to harden existing cyber fortification (block ports on firewalls, update anti-virus software with new signatures, etc.), or to withdraw (shutdown and/or disconnect the system or network). Defensive cyber weapons could be analogous to AAA or SAMs that are deployed around vital targets, or they could include interceptors that could "fly out" to shoot down the inbound aggressor. For example, existing virus or spam techniques could be used to quickly package and push out a "good" virus that can spread and self guide across the Internet to destroy malicious code. Such a weapon could be quickly developed and launched in response to an adversaries cyber weapons to counter and mitigate the destructive or disruptive effects. Another example would be to build the capability to "laser designate" adversary cyber weapons at their source to enable these defensive cyber weapons to target them on their inbound track. These weapons do pose legal and potential collateral damage challenges; however, these issues are not unlike those facing similar weapons in the other warfighting domains. Finally, these defensive cyber weapons do not have to be limited towards defense but could also be employed offensively.

d. Professionalizing the Force

Last but not least, future cyber forces must be properly trained and ready to fight during this future cyber war. This training becomes all the more challenging due to the high rate of technological advances and because industry is designed to build computer and network security experts vice cyber warfighters. Cyber warfighters must be experts in not only the technological aspects of computer and network security but must also be adept at military doctrine and tactics; they must be warfighters first and technicians second. As such, the DoD should stand up its own cyber warfare schools to grow this force. Robust cyber exercises should be integrated with all conventional exercises to ensure sufficient cyber forces are properly prepared to defend against a determined and capable adversary in this future cyberwar scenario. Advanced cyber weapons schools should also be stood up to develop cyber "Aces" who can return to the force and share their advanced cyber warfare techniques with their units. On a final note, the current trends of information technology outsourcing and core services centralization pose a threat to the ability of the DoD to maintain a viable and ready cyber force. Both options provide a more cost effective method of providing computer and network security services; however, both erode the professional cyber force that needs to be built to defend DoD and U.S. cyberspace.

2. Operational Command and Control

During the first cyberwar, it is reasonable to assume that any adversary would exploit seams and vulnerabilities to create competitive advantages on the battlefield. The implication is that a failure to have unity of effort on cyber defense among the Army, Navy, Air Force, and Marine Corps (or within each service) will translate into exploitable seams that will reduce the defensibility of friendly cyberspace. Therefore, integrated cyber defenses must be joint by definition in order to be effective.

Second, the best operational C2 structure for an effective integrated defense across joint forces is centralized control and decentralized execution. In this area, serious deficiencies exist across and within the services and between Combatant Commands (COCOM). For example, U.S. Strategic Command (STRATCOM) has been formally assigned the mission of defending the DoD' Global Information Grid and therefore

should have operational control (OPCON) of all cyber defense forces; however, geographic Combatant Commanders have been unwilling to yield OPCON to STRATCOM. Moreover, each geographic COCOM conducts CND differently, thereby creating seams in the defenses which adversary cyber forces can and will readily exploit. To further confuse the issue, each service conducts CND differently and has differing internal C2 structures. This effect creates multiple seams throughout DoD's cyber defenses. An example of this fractured operational C2 structure is illustrated in Figure 15. From the perspective of the communications squadron at Osan Air Base (AB), CND orders are tasked from multiple sources at multiple echelons, and it is not uncommon for these orders to be inconsistent or conflicting. Other AF installations in the Pacific Command (PACOM) AOR have a similarly convoluted operational C2 structure; in addition, Navy/Marine Corps and Army installations in the same AOR have comparably confusing C2 structures which differ between each service.

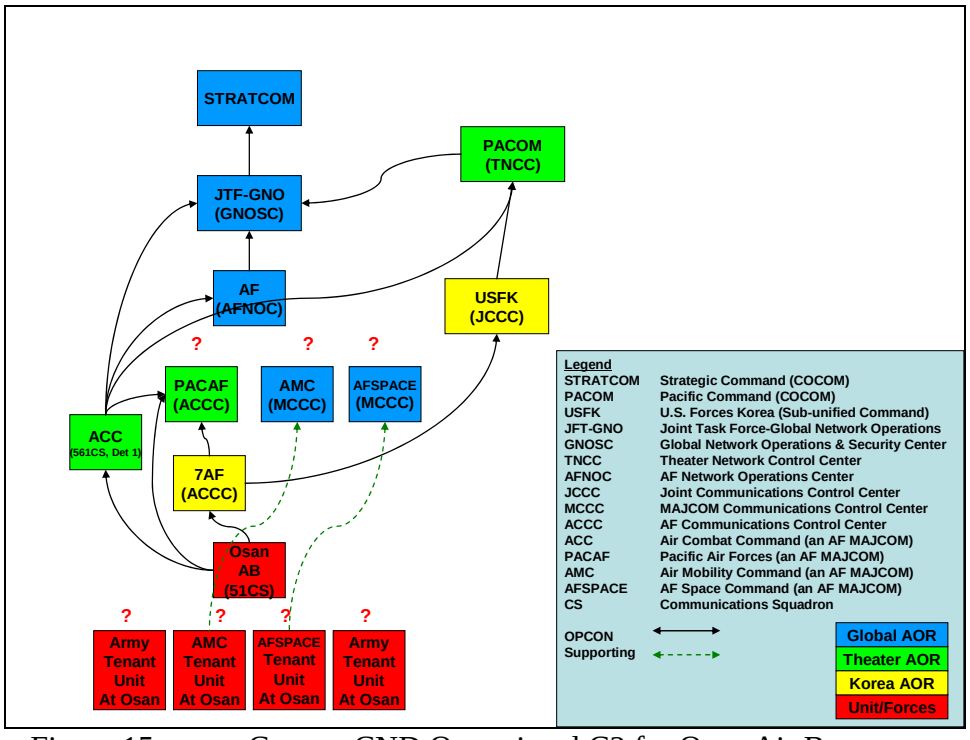


Figure 15. Current CND Operational C2 for Osan Air Base

Due to the inherent nature of networks to cross organizational boundaries, there are no easy solutions to simplifying this convoluted operational C2 structure. Since the Area of Responsibility (AOR) for defensive cyberspace operations is global (see Chapter II, section E.1.), cyber defense forces should be operationally organized to take this warfighting domain feature into account. Therefore, JTF-GNO should serve as the Area Cyber Defense Commander for global cyber defense operations in order to ensure joint and global unity of effort. Each service component should then present their respective service cyber defense forces in a unified C2 structure spanning the same global AOR. The next C2 echelon within each service should align their cyber forces along existing COCOM geographic boundaries. This echelon will report OPCON to the service component to maintain global unity of effort and would also serve as the theater cyber defense service component to the COCOM in a supporting relationship to their respective Theater Network Control Center (TNCC). Service cyber defense units at each base would fill the last C2 echelon; more importantly, any tenant units would report to the base cyber defense unit. For bases that host multiple services, the service that provides base operating support would provide the base's cyber defense C2, and all tenant units (regardless of service) would report to the base cyber defense unit. This operational C2 structure clarifies cyber defense responsibilities and supported/supporting command relationships. It also provides a hierarchical structure to enable coordinated operational-level planning and execution of DoD cyber defenses. This proposed operational C2 structure for CND is illustrated in Figure 16.

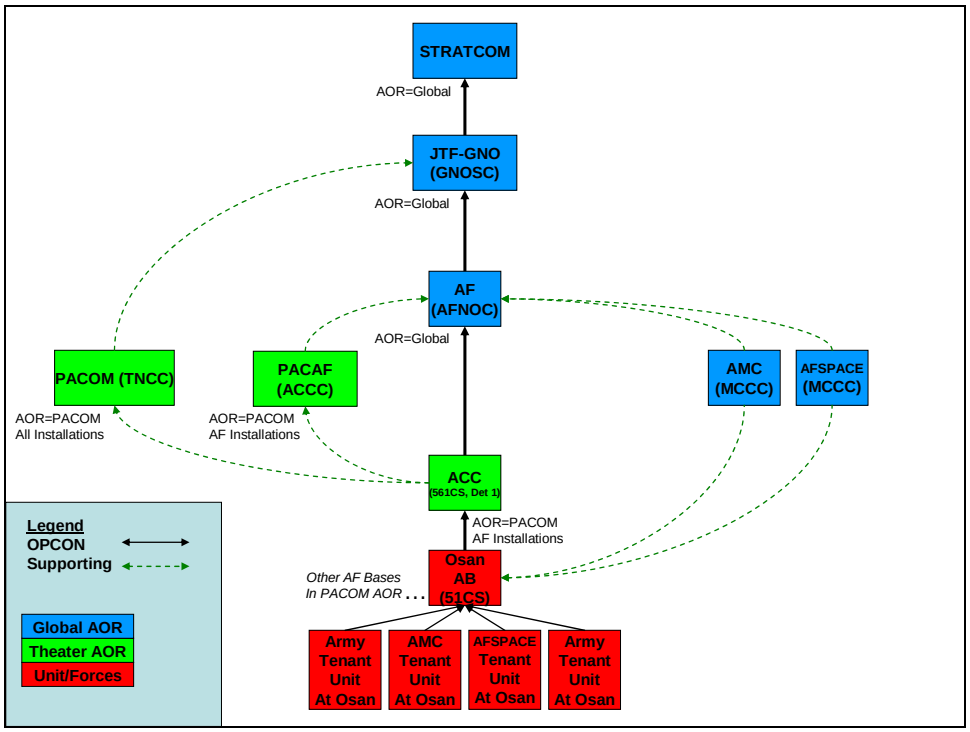


Figure 16. Proposed CND Operational C2

3. Operational Employment Concept

Along with technology and an organizational framework, a holistic operational concept and related military doctrine are required to translate tactical capabilities into operational-level leverage. Since the warfighting domain of cyberspace is not fundamentally different across services (see Chapter II, section E.6.), cyber defense doctrine should be joint to ensure unity of effort across all service. Using the RAF's successful employment of defensive air power and the EAF's failed employment of the same as a model, defensive doctrine can be broken down into three broad doctrinal functions: 1) to posture, 2) to maneuver, and 3) to recover. The model in Figure 17 provides an illustration. These functions can be applied to CND doctrine as well. The focus framework is primarily intended to apply to the operational level of war; however, this framework can also applicable at lower command echelons to provide tactical commanders a valuable tool to improve the defensibility and survivability of their assigned portions of cyberspace. Finally, an effective defense is not performed

sequentially; rather, each defense function should support the other two functions. Thus, the overall strength of one's defenses can be characterized by the balance and supporting overlap of defensive tasks across all three functions.

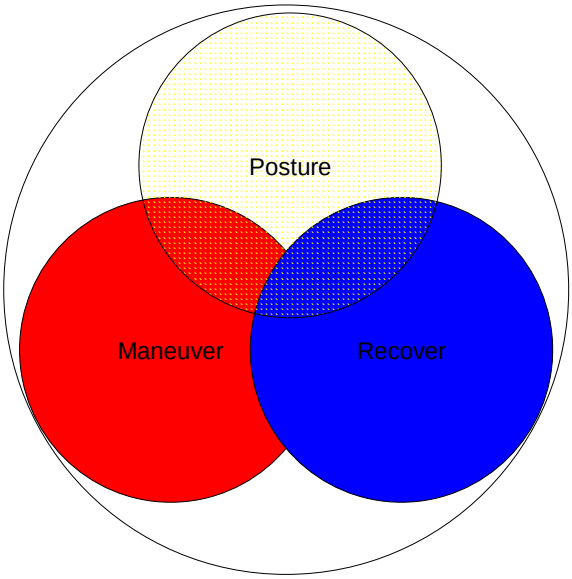


Figure 17. CND Doctrinal Functions

a. Posture

Posturing encompasses proactive and reactive actions that increase the survivability of forces in the event of an attack. The key principle behind posturing is anticipating cyber attacks and then planning and implementing measures to ensure the survivability of friendly combat power. Posturing can done reactively in response to conflict escalation. It can also be done proactively in preparation for friendly combat operations. Posturing tasks include the employment of cover, concealment, dispersal, camouflage, hardening, redundancy, and deception (e.g. decoys) in combination to increase the survivability of friendly cyberspace. Posturing assumes that attacks are to be expected and does not assume away an enemy's will or capability to initiate the attack. Therefore, friendly cyber defense forces should never be caught unprepared. Finally, posturing supports maneuver and recover by maximizing the combat power available for maneuver and minimizing the lost combat power that must be reconstituted.

b. Maneuver

The second doctrinal function for CND is maneuvering. Maneuver encompasses proactive and reactive actions taken in response to and during attacks. It also includes offensive and defensive maneuvers to engage with and/or retreat from the enemy. From the defensive perspective, the purpose of maneuvering is to preserve friendly combat power. During an attack, one of the most difficult steps is to develop an initial list of possible countermeasures in response. The basic maneuvering tasks provide this initial list of actions that can be taken during an attack, and this list includes attacking (the source), defending (fighting in place), relocating (moving to a more advantageous or less vulnerable portion of cyberspace like a redundant command-and-control node or to a more secure network), augmenting (to shore up defenses), withdrawing (shutting down or abandoning networks or systems), or delaying (any actions that buys time for friendly cyber forces to take other actions). Maneuver also implies that defenses should be dynamic and should not solely rely on static fortifications, as is the accepted methodology today. Cyber defenders must be creative and take the initiative in order to outmaneuver their attackers in cyberspace. Finally, maneuver supports posturing and recovery by further increasing the survivability of friendly combat power.

c. Recover

The final doctrinal function for CND is recovery. The recover function encompasses actions taken to recover and reconstitute combat capabilities. Recovery includes performing battle damage assessment (BDA), repairs, reconstitution, and emergency containment of extreme damage to mitigate its impact on the entire force. This step is vital to restoring maximum combat power as quickly as possible. Recovery is also dependent upon rear logistics support (spares, manpower, connectivity, bandwidth/throughput, etc.). Recovery supports posturing and maneuver by restoring friendly combat power.

Functions	Tasks
Posture	Cover
	Concealment
	Camouflage
	Hardening
	Deception (Decoys)
	Dispersal
	Redundancy
Maneuver	Attack
	Defend
	Relocate
	Augment
	Withdraw
	Delay
Recover	Battle Damage Assessment
	Containment
	Repair
	Reconstitution

Figure 18. CND Doctrinal Tasks

C. SUMMARY

The proper combination of technology employment, operational command and control, and operational employment are key to the development of an effective cyber defense capability. By combining the doctrinally significant attributes of the cyberspace warfighting domain and the doctrinal lesson of successful and failed air defense campaigns, this chapter recommends that the DoD invest resources towards the development of joint, integrated cyber defense capabilities analogous to historically successful integrated air defenses. Technology employment provides the tactical foundation upon which to build this capability; however, operational level C2 and operational level employment provide the doctrine necessary to translate tactical successes into operational leverage. Finally, the DoD is currently lacking in all three of these areas despite the fact that adversary states are investing in developing more powerful cyber warfare capabilities. The solution is clear: the DoD needs to properly invest in the development and employment of new technologies and the related organizational and doctrinal elements to fuse these technological capabilities into cyber combat power.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

This thesis has explored the doctrinal concepts needed to develop the proper technology, operational employment concepts, and operational command and control to build an effective integrated cyber defense capability for the DoD. By defining the basic attributes of the warfighting domain of cyberspace, this thesis established that the cyberspace domain has characteristics comparable to those of the air warfighting domain. Then by analyzing successful and failed defensive air campaigns of the past, an initial framework was developed to describe the necessary components of an effective integrated cyber defense capability.

The arena of cyber warfare, however, is still virgin territory. One purpose of this research was to provide an answer to the question of how the DoD should go about building a viable cyber defense capability; however, the more important purpose of this research was to provide a usable methodology by which to identify and ask the right doctrinal questions to glean these answers due to our limited real historical experience of conducting cyberwars. As such, this thesis looked at cyber defense through a conventional doctrine lens to tease out some doctrinal truths. Future research through an unconventional doctrinal lens may also provide useful insights for further developing DoD cyber defense capabilities. In addition, this thesis used the development of air power doctrine to ask and answer questions relating to cyber defense doctrine; however, the cyberspace domain also shares attributes with the sea, land, and space warfighting domains. Future research comparing cyberspace to these other domains may also reveal useful doctrinal or policy insights.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: KEY DOD AND SERVICE PUBLICATIONS

* Note: Please reference the "List of References" for complete bibliographical information on these sources.

A. DoD-level Publications:

- *DODI 5200.40: Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*
- *DODD 8500.1: Information Assurance (IA)*
- *DODI 8500.2: Information Assurance (IA) Implementation*
- *DODD 8530.1: Computer Network Defense*
- *DODI 8530.2: Support to Computer Network Defense (CND)*

B. CJCS-level Publications:

- *CJCSI 3401.03: Information Assurance (IA) and Computer Network Defense (CND)*
- *CJCSI 6510.01 Series: Information Assurance (IA) and Computer Network Defense (CND)*
- *CJCSM 6510.01: Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*
- *JP 3-13: Information Operations*
- *JP 3-13.1: Electronic Warfare*
- *JP 3-13.3: Operations Security*
- *JP 3-13.4: Military Deception*
- *JP 3-53: Joint Doctrine for Psychological Operations*
- *Joint Information Operations Planning Handbook*

C. Combatant Commander-level Publications:

- *SD 527-1: Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures*

D. Service-level Publications:

- *AFDD 2-5: Information Operations*
- *AFI 33-115 Volume 1: Network Operations*
- *AFI 33-202: Network and Computer Security*
- *FM 3-13: Information Operations Doctrine, Tactics, Techniques, and Procedures*
- *OPNAV INST 5239.1A: Department of the Navy Automatic Data Processing Security Program*
- *OPNAV INST 5239.3: Navy Implementation Department of Defense Intelligence Information System (DODIIS) Public Key Infrastructure (PKI)*
- *OPNAV INST 5450.231: Mission, Functions and Tasks of the Fleet Information Warfare Center (FIWC)*
- *MCWP 3-40.4: Marine Air Ground Task Force Information Operations*

APPENDIX B: KEY CYBER WARFARE PUBLICATIONS

* Note: Please reference the "List of References" for complete bibliographical information on these sources.

A. Strategic-level Publications:

- *Information Operations Roadmap (DECLASSIFIED)*, dated Oct 30, 2003
- Gregory Rattray's *Strategic Warfare in Cyberspace*
- *Information Warfare - Defense (IW-D)*
- Alan D. Campen's, et al. *Cyberwar: Security, Strategy, and Conflict in the Information Age*
- Arthur F. Galpin's *Computer Network Defense for the United States of America*
- Jacques S. Gansler's "Protecting Cyberspace." in Hans Binnendijk, ed., *Transforming America's Military*
- Robert H. Anderson's, et al. *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*

B. Operational-level Publications:

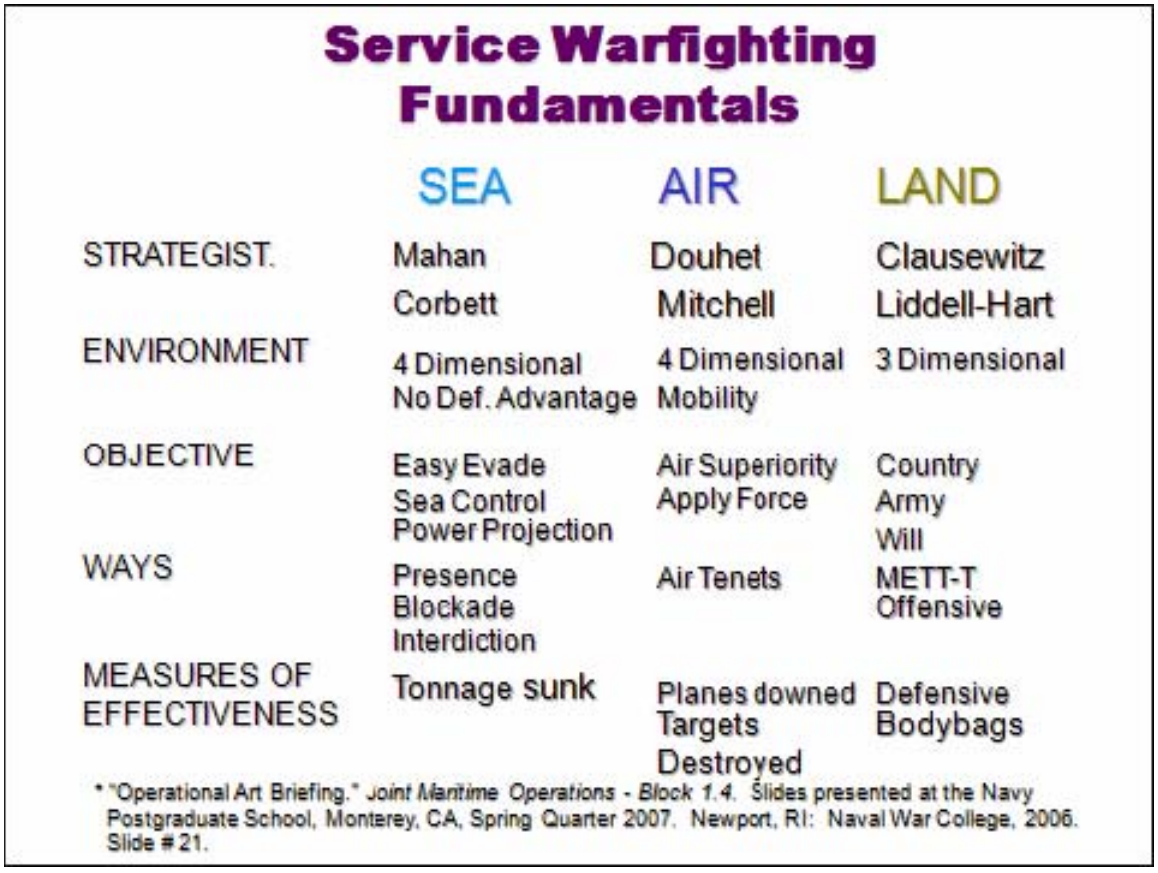
- Juan Vega's *Computer Network Operations Methodology*

C. Tactical/Technical-level Publications:

- Dorothy E. Denning's *Information Warfare and Security*
- RAND's *Advanced Network Defense Research*
- Peng Liu's, et al. *Trusted Recovery and Defensive Information Warfare*
- Eric J. Holdaway's *Active Computer Network Defense: An Assessment*
- Oren K. Upton's *Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspections*

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: SERVICE WARFIGHTING FUNDAMENTALS



Service Warfighting Fundamentals

	SEA	AIR	LAND
STRATEGIST.	Mahan Corbett	Douhet Mitchell	Clausewitz Liddell-Hart
ENVIRONMENT	4 Dimensional No Def. Advantage	4 Dimensional Mobility	3 Dimensional
OBJECTIVE	Easy Evade Sea Control Power Projection	Air Superiority Apply Force	Country Army Will
WAYS	Presence Blockade Interdiction	Air Tenets	METT-T Offensive
MEASURES OF EFFECTIVENESS	Tonnage sunk	Planes downed Targets Destroyed	Defensive Bodybags

* "Operational Art Briefing." *Joint Maritime Operations - Block 1.4.* Slides presented at the Navy Postgraduate School, Monterey, CA, Spring Quarter 2007. Newport, RI: Naval War College, 2006. Slide # 21.

Table 3. Service Warfighting Fundamentals (From [95])

[95] "Block 1.4: Operational Art Briefing," *Joint Maritime Operations*, slides presented at the Navy Postgraduate School, Monterey, CA, Spring Quarter 2007, Newport, RI: Naval War College, 2007, slide #21.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: MILITARY FORCES - BATTLE OF BRITAIN

Country	Combat Force Strength
Great Britain	Ground: 27 infantry divisions* 1 armor division with 963 tanks (103**) Sea: 36 Navy destroyers and 1,100 lesser sea craft Air: 749 fighters(507***) 151 bombers (84***)

Country	Combat Force Strength
Germany	Ground: 13 divisions (90,000 infantry + 30,000 airborne infantry)**** 650 tanks **** Air: 1055 fighters (824***) 1447 bombers (1017***)

Table 4. Military Force Strength - Battle of Britain[96]

* Most infantry divisions were at less than half of their manpower strength of 15,500 men and had only one-sixth of their required complement of field guns and anti-tank guns, as well as being short on armored vehicles and machine guns.

** Only 103 British tanks were capable of countering existing German armor.

*** Only 507 British fighters and 84 British bombers were serviceable. Only 824 German fighters and 1017 German bombers were serviceable.

**** The numbers include only the first wave forces committed to the invasion. Follow-on forces would bolster the number of ground forces to 260,000 men in 41 divisions, to include 30 infantry, 6 Panzer, 3 motorized, and 2 airborne divisions.

[96] Richard Overy, *The Battle of Britain: The Myth and the Reality*, 159-161.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E: AIR ORDER OF BATTLE - BATTLE OF BRITAIN

Country	Combat Aircraft*		Combat Aircraft Losses		Aircraft Production (Fighters Only)	
United Kingdom (Royal Air Force [RAF])	463 Hurricanes	(347)	July	76	July	496
	286 Spitfires	(160)	Aug	329	Aug	476
	37 Defiants	(25)	Sep	350	Sep	717
	114 Blenheims	(59)	Oct	130	Oct	~420
	Total: 900	**(591)**	**Total:**	885	**Total:**	**~2102**
Grand Total	***900 (591)***		***885***		***~2102***	

Country	Combat Aircraft*		Combat Aircraft Losses		Aircraft Production (Fighter Only)	
Germany (Luftwaffe)	809 Me-109	(656)				
	246 Me-110	(168)	July	190	July	~150
	316 Ju-87	(248)	Aug	546	Aug	~150
	1131 Ju-88/		Sep	477	Sep	~150
	He-111/Do-17	(769)	Oct	259	Oct	~150
	Total: 2502	**(1841)**	**Total:**	1472	**Total:**	~600
Grand Total	***2502 (1841)***		***1472***		***~600***	

Table 5. Air Order of Battle (Combat Aircraft Only) - Battle of Britain (After [97])

* Note that these numbers include only combat aircraft since non-combat aircraft have limited to no utility in providing air superiority. Also, the numbers in parentheses represent the number of serviceable aircraft out of the total.

Month	RAF**	Luftwaffe**
July	1,482	906
Aug	1,456	869
Sept	1,558	735
Oct	1,662	673
Average (Trend)	1,540 (+60 per month)	796 (-78 per month)

Table 6. Single-Engine Fighter Pilot Strength - RAF versus Luftwaffe (After [98])

** Based upon number of pilots available at or near the beginning of each month.

[97] Len Deighton, *Battle of Britain*,. 92, 96-97, 101, 115, 149, 165, 167-168, 172-173, and 199; Richard Overy, *The Battle of Britain: The Myth and the Reality*, 35-37, 159-161; and Frank Heilenday, *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*, 3-4.

[98] Richard Overy, *The Battle of Britain: The Myth and the Reality*, 162.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F: MILITARY FORCES - SIX DAYS WAR

Country	Combat Force Strength	Combat Losses
Israel	264,000 troops 800 tanks 300 planes	2,000 troops unknown 40 planes (13% loss)
Grand Total	***264,000 troops*** ***800 tanks*** ***300 planes***	***2,000 (1% loss)*** ***unknown*** ***40 planes (13% loss)***

Country*	Combat Force Strength	Combat Losses
Egypt	240,000 troops 1,200 tanks 580 planes	80K-100K troops (>33% loss) 700-800 tanks (58% loss) 431 planes (74% loss)
Syria	50,000 troops 400 tanks 136 planes	1,000 (< 1% loss) unknown 59 planes (43% loss)
Jordan	50,000 troops 200 tanks 40 planes	5,000 (8% loss) unknown 19 plans (48% loss)
Grand Total	***340,000 troops*** ***1,800 tanks*** ***756 planes***	***80K-100K troops (>24% loss)*** ***700-800 tanks (>39% loss)*** ***509 planes (67% loss)***

Table 7. Military Force Strength - Six Days War (After [99])

* Note: Force numbers for Iraq, Algeria, Kuwait, and Saudi Arabia have been purposefully excluded because their respective forces were never fully committed to combat.

[99] "Armed Conflict Events Data: The Six Days War," *On War.com*, http://onwar.com/aced/data/9999/6day1967.htm, last accessed Oct 15, 2007; Hal Kosut, ed., *Israel and the Arabs: The June 1967 War*, 67; and "The EAF History," http://www.geocities.com/egyptianairforce/history.html, last accessed Oct 15, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G: AIR ORDER OF BATTLE - SIX DAYS WAR

Country	Size of AF	Combat Aircraft**	Combat Aircraft Losses (after first two days)
Israel (Israeli Air Force [IAF])	8,000	72 Mirage III CJs 25 Vautour IIAs 20 Super Mystere B2s 40 Mystere IVs 40 Ouragans 60 Fouga Magisters **Total: 257**	6 Mirage III CJs 5 Vautour IIAs 0 Super Mystere B2s 9 Mystere IVs 4 Ouragans 6 Fouga Magisters **Total: 30 (12% loss)**
Grand Total	***8,000***	***257***	***30 (12% loss)***

Country*	Size of AF	Combat Aircraft**	Combat Aircraft Losses (after first two days)
Egypt (Egyptian Air Force [EAF])	20,000	30 Tu-16s 35-40 Il-28s 130 MiG-21s 80 MiG-19s 100 MiG-17s 50 MiG-15s 20-66 Su-7Bs **Total: 445-496**	30 Tu-16s 29 Il-28s 100 MiG-21s 29 MiG-19s 89 MiG-17s & MiG-15s 14 Su-7s **Total: 291 (59-65% loss)**
Syria (Syrian Air Force)	9,000	6 Il-28s 20 MiG-21s 20 MiG-19s 60 MiG-17s/15s **Total: 106**	2 Il-28s 33 MiG-21s/19s 23 MiG-17s/15s **Total: 58 (55% loss)**
Jordon (Jordanian Air Force)	2,000	21 Hunter MK6s **Total: 21**	21 Hunter MK6s **Total: 21 (100% loss)**
Grand Total	***31,000***	***576-623***	***370 (59-64% loss)***

Table 8. Air Order of Battle (Combat Aircraft Only) - Six Days War (After [100])

* Note: Force numbers for Iraq, Algeria, Kuwait, and Saudi Arabia have been purposefully excluded because their respective air forces were never fully committed to combat.

** Note that these numbers include only combat aircraft since non-combat aircraft have limited to no utility in providing air superiority.

[100] Trevor N. Dupuy, *Elusive Victory: The Arab-Israeli Wars, 1947-1947*, Dubuque, IA: Kendall/Hunt Publishing Company, 1992, 333; le Moniteur de l'Aeronautique 1966-67 in Rodney S. Crist, *Air Superiority: A Case Study*, Newport, RI: Naval War College, 1988, 25; Hal Kosut, ed., *Israel and the Arabs: The June 1967 War*, 67; "Arab-Israeli Aircraft Losses," http://www.geocities.com/CapeCanaveral/Hangar/2848/losses.htm, last accessed Oct 25, 2007; and "The EAF History," http://www.geocities.com/egyptianairforce/history.html, last accessed Oct 15, 2007. Note that the original chart was derived from Ronald D. Jones, *Israeli Air Superiority in the 1967 Arab-Israeli War: An Analysis of Operational Art*, Newport, RI: Naval War College, 1996,. 16-17; however, I went back to Jones' sources and corrected several errors.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"1967 Middle East War." *BBC News*. http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457035/html/default.stm. Last accessed Oct 25, 2007.

"5 June 1967 Israeli Air Strikes." *War and Game*, http://warandgame.blogspot.com/2007/10/5-june-1967-israeli-air-strikes.html. Last accessed Oct 15, 2007.

Advanced Network Defense Research. Santa Monica, CA: RAND, 2000.

Air Force Doctrine Document (AFDD) 2-5: Information Operations. Jan 11, 2005. Washington, DC: Air Force Publishing, 2005. http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5/afdd2-5.pdf. Last accessed Feb 6, 2007.

Air Force Instruction (AFI) 33-115 Volume 1: Network Operations (NetOps). May 24, 2006. Washington, DC: Air Force Publishing, 2006. http://www.e-publishing.af.mil/pubfiles/af/33/afi33-115v1/afi33-115v1.pdf. Last accessed Feb 6, 2007.

AFI 33-202: Network and Computer Security. Feb 3, 2006. Washington, DC: Air Force Publishing, 2006. http://www.e-publishing.af.mil/pubfiles/af/33/afi33-202v1/afi33-202v1.pdf. Last accessed Feb 6, 2007.

AF Operational Concept - Cyberwarfare (DRAFT). Apr 1, 2007. San Antonio, TX: 67th Network Warfare Wing.

Anderson, Robert H.; Phillip M. Feldman; Scott Gerwehr; Brian Houghton; Richard Mesic; John Pinder; Jeff Rothenberg; and James Chiesa. *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*. Santa Monica, CA: RAND, 2003. http://www.rand.org/pubs/monograph_reports/MR993/. Last accessed Feb 20, 2007.

"Arab Air Forces on 5 June 1967." *ACIG Journal*. http://www.acig.org/artman/publish/article_262.shtml. Last accessed Oct 15, 2007.

"Arab-Israel Six Days War: Intelligence Memorandum Prepared in the Central Intelligence Agency, May 26, 1967." http://www.zionism-israel.com/hdoc/CIA_on_War_Estimate_1967.htm. Last accessed Oct 25, 2007.

"Arab-Israeli Aircraft Losses," http://www.geocities.com/CapeCanaveral/Hangar/2848/losses.htm, last accessed Oct 25, 2007.

"Armed Conflict Events Database: The Six Days War." *On War.com*, http://onwar.com/aced/data/9999/6day1967.htm. Last accessed Oct 15, 2007.

Arquilla, John and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.

———. *Swarming and the Future of Conflict*. Santa Monica, CA: RAND, 2000.

Bickers, Richard T. *The Battle of Britain: The Greatest Battle in the History of Air Warfare*. New York, NY: Prentice Hall Press, 1990.

The Battle of Britain Historical Society. http://www.battleofbritain.net. Last accessed Feb 6, 2007.

The Battle of Britain History Site. http://www.raf.mod.uk/bob1940/bobhome.html. Last accessed Feb 6, 2007.

"The Battle of Britain Toolkit." (Air Command and Staff College Project 97-0564.01 updated Apr 28, 2001). *Air Command and Staff College Distance Learning CD version 3.2*. Maxwell AFB, AL: Air University Press, 2003.

Bauxbaum, Peter A. "Air Force Explores the Next Frontier." *GCN Magazine*, Feb 19, 2007 reprinted in *U.S. Air Force Aim Points*, Feb 21, 2007. http://aimpoints.hq.af.mil/display.cfm?id=16792. Last accessed Feb 21, 2007.

Bergquist, Ronald E. *The Role of Airpower in the Iran-Iraq War*. Maxwell AFB, AL: Air University Press, 1988.

Billo, Charles and Welton Chang. *Cyberwarfare: An Analysis of Means and Motivations of Selected Nation States*. Hanover, NH: Dartmouth College Press, 2004.

"Block 1.4: Operational Art Briefing." *Joint Maritime Operations.* Slides presented at the Navy Postgraduate School, Monterey, CA, Spring Quarter 2007. Newport, RI: Naval War College, 2007.

Bowen, Jeremy. *Six Days: How the 1967 War Shaped the Middle East*. New York, NY: Thomas Dunne Books, 2005.

British Air Ministry. *The Battle of Britain*. New York, NY: Garden City Publishing Co., Inc., 1941.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Gooden, eds. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: Armed Forces Communications Electronics Association International Press, 1996.

Chairman of the Joint Chiefs of Staff (CJCS) Instruction (CJCSI) 3401.03: Information Assurance (IA) and Computer Network Defense (CND). July 15, 2003. Washington, DC: Office of the Chairman, Joint Chiefs of Staff, 2003. http://www.dtic.mil/cjcs_directives/cdata/unlimit/3401_03.pdf. Last accessed Feb 16, 2007.

CJCSI 6510.01 Series: Information Assurance (IA) and Computer Network Defense (CND). Jun 15, 2004. Washington, DC: Office of the CJCS, 2004. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf. Last accessed Feb 20, 2007.

CJCS Manual (CJCSM) 6510.01: Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND). Mar 25, 2003 (with changes 1-3 dated through Mar 8, 2006). Washington, DC: Office of the CJCS, 2003. http://www.dtic.mil/cjcs_directives/cjcs/manuals.htm. Last accessed Feb 20, 2007.

Cooling, Benjamin F., ed. *Case Studies in the Achievement of Air Superiority*. Washington, DC: Air Force History & Museums Program, 1994.

Crist, Rodney S. *Air Superiority: A Case Study*. Newport, RI: Naval War College, 1988.

Deighton, Len. *Battle of Britain*. London, UK: George Rainbird Limited, 1980.

Denning, Dorothy E. *Information Warfare and Security*. Berkeley, CA: ACM Press Books, 1999.

———. "Reflections on Cyberweapons Controls." *Computer Security Journal*, XVI, 4, Fall 2000. 43-53.

DoD Instruction (DODI) 5200.40: Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Dec 30, 1997. Washington, DC: Office of the Secretary of Defense, 1997. http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf. Last accessed Feb 16, 2007.

DoD Directive (DODD) 8500.1: Information Assurance (IA). Oct 24, 2002. Washington, DC: Office of the Secretary of Defense, 2002. http://www.dtic.mil/whs/directives/corres/pdf/850001_102402/850001p.pdf. Last accessed Feb 16, 2007.

DODI 8500.2: Information Assurance (IA) Implementation. Feb 6, 2003. Washington, DC: Office of the Secretary of Defense, 2003. http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf. Last accessed Feb 16, 2007.

DODD 8530.1: Computer Network Defense. Jan 8, 2001. Washington, DC: Office of the Secretary of Defense, 2002. http://iase.disa.mil/policy.html. Last accessed Feb 20, 2007.

DODI 8530.2: Support to Computer Network Defense (CND). Mar 9, 2001. Washington, DC: Office of the Secretary of Defense, 2002. http://iase.disa.mil/policy.html. Last accessed Feb 20, 2007.

Dupuy, Trevor N. *Elusive Victory: The Arab-Israeli Wars, 1947-1947*. Dubuque, IA: Kendall/Hunt Publishing Company, 1992.

"The EAF History." http://www.geocities.com/egyptianairforce/history.html. Last accessed Oct 15, 2007

"Egyptian SA-2 Photo" *Egyptian National Military Museum*. http://www.richard-seaman.com/Aircraft/Museums/EgyptianNationalMilitaryMuseum/index.html. Last accessed Oct 26, 2007.

Field Manual (FM) 3-13: Information Operations Doctrine, Tactics, Techniques, and Procedures. Washington, DC: Department of the Army, 2003.

Fortification. Dictionary.com. *Dictionary.com Unabridged (v 1.1)*. Random House, Inc. http://dictionary.reference.com/browse/fortification. Last accessed Sept 9, 2007.

Galland, Adolph. "Defeat of the Luftwaffe: Fundamental Causes." *Air University Quarterly Review*, VI-1: 8-36: Spring 1953.

Galpin, Arthur F. *Computer Network Defense for the United States of America*. Carlisle Barracks, PA: U.S. Army War College, 2002.

Gansler, Jacques S. "Protecting Cyberspace." in Hans Binnendijk, ed., *Transforming America's Military*. Washington, DC: National Defense University, 2002. 331-344.

Glazer, Thomas E. *The 1967 Arab-Israeli Six-Day War: An Analysis Using the Principles of War*. Newport, RI: Naval War College, 2001.

Gleave, T.P. "The Battle of Britain: Strategy, Tactics, Atmosphere." *Flight International*, September 16, 1965. 494-502.

Gunnersen, Stanley S. *A Study of Airpower Employment in the Six Days War*. Maxwell AFB, AL: Air University, 1971.

Gibson, William. *Neuromancer*. New York, NY: Ace Books, 1984.

"HAWK." *FAS Military Network*. http://www.fas.org. Last accessed Oct 15, 2007.

"HAWK." *Israeli Weapons.com*. http://www.israeli-weapons.com/weapons/missile_systems/surface_missiles/hawk/Hawk.htm. Last accessed Oct 26, 2007.

"HAWK Missile B-7-5: History of the Hawk Missile System." http://www.geocities.com/hawkmissileb75/history.htm?200726. Last accessed Oct 25, 2007.

Harris, Stephen John and Higham, Robin D. S. *Why Air Forces Fail: The Anatomy of Defeat*. Lexington, KY: University Press of Kentucky, 1996.

Heilenday, Frank W. *The Battle of Britain -- Luftwaffe vs. RAF: Lessons Learned and Lingering Myths from World War II (P-7915)*. Santa Monica, CA: RAND, 1995.

Heiman, Leo. "Soviet Air Tactics—No Room for Initiative." *Air Force Magazine*, 51, Aug 1968. 42-45.

Higham, Robin. "The Arab Air Forces" in Robin Higham and Stephen J. Harris, eds. *Why Air Forces Fail: The Anatomy of Defeat*, Lexington, KY: University Press of Kentucky, 2006.

Holdaway, Eric J. *Active Computer Network Defense: An Assessment*. Maxwell AFB, AL: Air University, 2001

Holmes, Erik. "Wynne Pleased with Tanker 'Horse Race.'"*Air Force Times.* Feb 26, 2007. 10.

Hough, Richard. *The Battle of Britain: The Greatest Air Battle of World War II*. New York, NY: W.W. Norton, 1989.

Information Operations Roadmap (DECLASSIFIED), Oct 30, 2003. http://freegovinfo.info//node/913. Last accessed Feb 6, 2007.

Information Warfare - Defense (IW-D). Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, 1996.

"The Israeli Navy Throughout Israel's Wars." *Jewish Virtual Library*. http://www.jewishvirtuallibrary.org/jsource/Society_&_Culture/navywar.html. Last accessed Oct 15, 2007.

James, T.C.G. *The Battle of Britain (Air Defense of Great Britain; vol. 2)*. New York, NY: Frank Cass Publishers, 2000.

Joint Information Operations Planning Handbook. January 2007. Norfolk, VA: Joint Forces Staff College, 2007.

Joint Publication (JP) 1-02: Department of Defense (DoD) Dictionary of Military and Associated Terms. Apr 12, 2001 (as amended through Jul 12, 2007). Washington, DC: Office of the CJCS, 2007. http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. Last accessed Sept 11, 2007.

JP 3-13: Information Operations. Feb 13, 2006. Washington, DC: Office of the CJCS, 2006. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. Last accessed Feb 6, 2007.

JP 3-13.1: Electronic Warfare. Jan 25, 2007. Washington, DC: Office of the CJCS, 2007. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_1.pdf. Last accessed Oct 1, 2007.

JP 3-13.3: Operations Security. Jun 29, 2006. Washington, DC: Office of the CJCS, 2006. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_3.pdf. Last accessed Oct 1, 2007.

JP 3-13.4: Military Deception. Jul 13, 2006. Washington, DC: Office of the CJCS, 2006. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_4.pdf. Last accessed Oct 1, 2007.

JP 3-53: Joint Doctrine for Psychological Operations, Sept 5, 2003. Washington, DC: Office of the CJCS, 2003. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53print.pdf. Last accessed Oct 1, 2007.

Jones, Ronald D. *Israeli Air Superiority in the 1967 Arab-Israeli War: An Analysis of Operational Art*. Newport, RI: Naval War College, 1996.

"The June 1967 War." *Egypt Country Studies*. Washington, DC: Library of Congress, 1990. http://lcweb2.loc.gov . Last access Feb 25, 2007.

"June 1967 War." *Israel Country Studies*. Washington, DC: Library of Congress, 1988. http://lcweb2.loc.gov . Last access Feb 25, 2007.

"June 1967 War and Aftermath." *Jordan Country Studies*. Washington, DC: Library of Congress, 1989. http://lcweb2.loc.gov . Last access Feb 25, 2007.

Kenyon, Henry S. "Task Force Explores New Military Frontier." *Signal Magazine*, Vol. 61, No. 2, Oct 2006. 55-57.

Kosut, Hal, ed. *Israel and the Arabs: The June 1967 War*. New York, NY: Facts on File Publications, 1968.

Kreis, John F. *Air Warfare and Air Base Air Defense, 1914-1973*. Washington, DC: Office of Air Force History, U.S. Air Force, 1988.

Libicki, Martin C. *Defending Cyberspace and Other Metaphors*. Washington, DC: National Defense University, 1997.

———. *What is Information Warfare*. Washington, DC: National Defense University, 1995.

Liu, Peng and Sushil Jajodia. *Trusted Recovery and Defensive Information Warfare*. Boston, MA: Kluwer Academic Publishers, 2002.

Lopez, C. Todd (SSgt, USAF). "Fighting in Cyberspace Means Cyber Domain Dominance.", *AF Print News*, Feb 28, 2007. http://www.af.mil/news/story.asp?id=123042670. Last accessed Sept 11, 2007.

Marine Corps Warfighting Publication (MCWP) 3-40.4: Marine Air Ground Task Force Information Operations. Quantico, VA: Marine Corps Combat Development Command, 2003.

"MiG-21 Specifications." *FAS Military Network*. http://www.fas.org. Last accessed Oct 15, 2007.

"MiG-21 Specifications." *Combat Aircraft.com*. http://www.combataircraft.com. Last accessed Oct 15, 2007.

"Military Capabilities of Israel and the Arab States." May 26, 1967. Washington, DC: Central Intelligence Agency. http://www.sixdaywar.co.uk/graphics/arab-israeli_memo.jpg. Last accessed Oct 25, 2007.

"Mirage III Specifications." *FAS Military Network*. http://www.fas.org. Last accessed Oct 15, 2007.

"Mirage III Specifications." *Combat Aircraft.com*. http://www.combataircraft.com. Last accessed Oct 15, 2007.

Monsarrat, John. "Radar in Retrospect, How It Helped Win the Battle of Britain and the Battle of Okinawa." *Journal of Electronic Defense*, 14-10, October 1991, 92-100.

Mutawi, Samir A. *Jordan in the 1967 War*. Cambridge, MA: Cambridge University Press, 1987.

National Strategy to Secure Cyberspace, Feb 2003. Washington, DC: White House, 2006. http://www.whitehouse.gov/pcipb/. Last accessed Feb 6, 2007.

Nordeen, Lon O., Jr. *Air Warfare in the Missile Age*. Washington, DC: Smithsonian Institution Press, 2002. 111-123

Operational Navy Instruction (OPNAV INST) 5239.1A: Department of the Navy Automatic Data Processing Security Program. Washington, DC: Office of the Chief of Naval Operation, 1982.

OPNAV INST 5239.3: Navy Implementation Department of Defense Intelligence Information System (DODIIS) Public Key Infrastructure (PKI). Washington, DC: Office of the Chief of Naval Operation, 2006.

OPNAV INST 5450.231: Mission, Functions and Tasks of the Fleet Information Warfare Center (FIWC). Washington, DC: Office of the Chief of Naval Operation, 1995.

"Operation Moked: Destruction of Arab Air Forces." *ACIG Journal*, http://www.acig.org/artman/publish/article_260.shtml. Last accessed Oct 15, 2007.

Oren, Michael. *Six Days of War: June 1967 and the Making of the Modern Middle East*. Oxford, UK: Oxford University Press, 2002.

Overy, Richard. *The Battle of Britain: The Myth and the Reality*. New York, NY: W.W. Norton & Company, 2000.

"OSI Model." *Huffman Reference Materials*. http://www.huffmanreference.com/pdf_download.html. Last accessed Nov 20, 2007.

Pingel, Thomas J. "Key Defensive Terrain in Cyberspace: A Geographic Perspective." *Proceedings of the 2003 International Conference on Politics and Information Systems: Technologies and Applications*, Orlando, FL, 2003, 159-163. http://www.geog.ucsb.edu/~pingel/. Last accessed Aug 6, 2007.

Planning Considerations for Defensive Information Warfare - Information Assurance. Falls Church, VA: Defense Information Systems Agency, 1993.

Poisel, Richard A. *Introduction to Communication Electronic Warfare Systems*. Boston, MA: Artech House, 2002.

Pollack, Kenneth M. "Air Power in the Six-Day War." *Journal of Strategic Studies*, 28, Jun 2005. 471-503.

———. *Arabs at War: Military Effectiveness, 1948-1991*. Lincoln, NE: University of Nebraska Press, 2002.

Preston, David L. "The Key to Victory: Fighter Command and the Tactical Air Reserves During the Battle of Britain." *Air Power History*, 41-4: Winter 1994.

Quadrennial Defense Review Press Briefing. Feb 3, 2006. Washington, DC: Office of the Secretary of Defense, 2006. http://www.defenselink.mil/qdr/. Last accessed Feb 8, 2006.

Quadrennial Defense Review Report. Feb 6, 2006. Washington, DC: Office of the Secretary of Defense, 2006. http://www.defenselink.mil/qdr/. Last accessed Feb 8, 2006.

Rattray, Gregory. "Improving the Nation's Cyber Defense." Aug 2006. http://www.bmcaoc.org/pdf/Rattray-CyberDefense.pdf. Last accessed Feb 6, 2007.

———. *Strategic Warfare in Cyberspace*. Cambridge, MA: The MIT Press, 2001.

———. "Securing Cyberspace." Spring 2004. http://www.pirp.harvard.edu/chttp://www.pirp.harvard.edu/courses/ISP483_Spring2004/RattrayCybersecurity%20-%20Spring%2004.ppt. Last accessed Feb 6, 2007.

"SA-2 GUIDELINE." *FAS Military Network*. http://www.fas.org. Last accessed Oct 15, 2007.

"Satellite Image - Sinai Peninsula." *Google Maps*. http://maps.google.com/maps?f=q&hl=en&geocode=&time=&date=&ttype=&q=egypt&ie=UTF8&ll=29.625996,33.97522&spn=4.048669,6.954346&t=h&z=8&om=1. Last accessed Oct 25, 2007.

Strategic Command Directive 527-1 (SD 527-1): Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures. Jan 27, 2006. Offutt Air Force Base, NE: Headquarters U.S. Strategic Command (USSTRATCOM), 2006. https://infosec.navy.mil/pub/docs/documents/dod/dodd/stratcom_d527-011_infocon_20060127.pdf. Last accessed Feb 16, 2007.

Teehan, Rita. *Data Security Breeches: Context and Incident Summaries*. Updated May 7, 2007. Washington, DC: Congressional Research Service, 2007.

Terrain. Dictionary.com. *WordNet® 3.0*. Princeton University. http://dictionary.reference.com/browse/terrain. Last accessed Sept 10, 2007.

Townsend, Peter. *Duel of Eagles: The Greatest Book on the Battle of Britain Ever Written*. Edison, NY: Castle Books, 2003.

TITAN RAIN Forensic Analysis Report. Joint Task Force-Global Network Operations. (Note: source document is classified)

TITAN RAIN Forensic Analysis Briefing. Joint Task Force-Global Network Operations. (Note: source document is classified)

Trenchard, Hugh Monttague. "Air Power and National Security." *Royal Air Force Pamphlet*. August 1946.

———. "The Principles of Air Power in War." *Air Power, Three Papers by the Viscount Trenchard*, Paper Two: 18-28: May 1945.

Upton, Oren K. *Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspections*. Monterey, CA: Navy Postgraduate School, 2003.

Vega, Juan Carlos. *Computer Network Operations Methodology*. Monterey, CA: Navy Postgraduate School, 2004.

Vego, Milan. *Operational Warfare*. Newport, RI: Naval War College, 2000.

Weapon. Dictionary.com. *Kernerman English Multilingual Dictionary*. K Dictionaries Ltd. http://dictionary.reference.com/browse/weapon. Last accessed Sept 9, 2007.

Wearden, Graeme. "Price of Cybercrime Tools Shrinks." *ZDNet*, Feb 9, 2007. http://news.zdnet.com/2100-1009_22-6158025.html . Last accessed Feb 16, 2007.

Waltz, Edward. *Information Warfare: Principles and Operations*. Boston, MA: Artech House, 1998.

Wilson, Clay. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. Updated Jun 5, 2007. Washington, DC: Congressional Research Service, 2007.

———. *Network Centric Operations: Background and Oversight Issues for Congress*. Updated Mar 15, 2007. Washington, DC: Congressional Research Service, 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. AFIT/ENEL
   ATTENTION: Capt James Ray or Ms. Kristy Aler
   Wright-Patterson AFB, Ohio

4. Professor Daniel Moran
   Naval Postgraduate School
   School of International Graduate Studies
   Monterey, California

5. Professor Dorothy Denning
   Naval Postgraduate School
   School of Operational and Information Sciences
   Monterey, California

6. Professor Maria Rasmussen
   Naval Postgraduate School
   School of International Graduate Studies
   Monterey, California

7. Joint Task Force Global Network Operations (JTF-GNO)
   Defense Information Systems Agency (DISA)
   Falls Church, Virginia

8. Air Force Network Operations Center (AFNOC)
   Air Force Cyber Command
   Barksdale AFB, Louisiana